Consumer-Facing Technology Fraud: Economics, Attack Methods and Potential Solutions☆

Mohammed Aamir Ali[a], Muhammad Ajmal Azad[b,*], Mario Parreno Centeno[a], Feng Hao[c], Aad van Moorsel[a]

[a] *School of Computing, Newcastle University, Newcastle Upon Tyne, United Kingdom*
[b] *Department of Computer Science and Mathematics, The University of Derby, Derby, United Kingdom*
[c] *Department of Computer Science, The University of Warwick, Coventry, United Kingdom*

Abstract

The emerging use of modern technologies has not only benefited society but also attracted fraudsters and criminals to misuse the technology for financial benefits. Fraud over the Internet has increased dramatically, resulting in an annual loss of billions of dollars to customers and service providers worldwide. Much of such fraud directly impacts individuals, both in the case of browser-based and mobile-based Internet services, as well as when using traditional telephony services, either through landline phones or mobiles. It is important that users of the technology should be both informed of fraud, as well as protected from frauds through fraud detection and prevention systems. In this paper, we present the anatomy of frauds for different consumer-facing technologies from three broad perspectives - we discuss Internet, mobile and traditional telecommunication, from the perspectives of losses through frauds over the technology, fraud attack mechanisms and systems used for detecting and preventing frauds. The paper also provides recommendations for securing emerging technologies from fraud and attacks.

Keywords: Consumer Frauds, Card Payment Frauds, Mobile Payment Frauds, Telecommunications Fraud, Fraud Economics, Fraud Mechanism

1. Introduction

The Internet today has reached a stage where many aspects of our lives are connected online, which includes buying products and services, doing businesses, banking, booking, managing of traveling and vacations and more. The advances in Internet technology have also greatly empowered criminals to misuse the technology for financial frauds [1]. The Internet has made it possible for cybercriminals to commit crimes at a distance of thousands

*Corresponding Author

Email addresses: m.a.ali2@ncl.ac.uk (Mohammed Aamir Ali), m.azad@derby.ac.uk (Muhammad Ajmal Azad), m.parreno-centeno1@ncl.ac.uk (Mario Parreno Centeno), feng.hao@warwick.ac.uk (Feng Hao), aad.vanmoorsel@ncl.ac.uk (Aad van Moorsel)

Table 1: Regional distribution of cybercrime for the year 2017 [2].

Region (World Bank)	**Region GDP (USD, trillions)**	**Cybercrime Cost (USD, billions)**	**Cybercrime Loss (%GDP)**
North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America & the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
MENA	3.1	2 to 5	0.06 to 0.16%
World	**$75.8**	**$445 to $608**	**0.59 to 0.80%**

of miles away, in another jurisdiction, hiding their identities and beyond the reach of any prosecutor. Cyber frauds result in a loss of around $608 billion to consumers, enterprises, and governments across the world [2].

Table 1 shows the regional distribution of cybercrime measured for the year 2017 [2]. In recent years, the cost of global cybercrime has increased from $445 billion in 2014 to $608 billion in 2017 [2]. Table 1 also compares regional GDP with the percentage loss in GDP as a result of cybercrime. It can be derived from the table that the higher the regional GDP, the greater are the losses associated with the cybercrime. The cybercriminals can use a number of ways to defraud the user of technology. They can use stolen personal information to apply for debit, credit and store cards; they can acquire such information via social engineering and phishing attacks using telephone and web (email, social networks). A recent report published by Symantec revealed that 978 million people in 20 countries were affected by cybercrime in 2017 [3]. These frauds resulted in a loss of $172 billion (an average of $142 per victim) to the consumers. Furthermore, the report also revealed that consumers spend nearly 24 hours on average dealing with the aftermath. Additionally, these frauds not only bring financial loss but also leave the psychological and social effects on the well-being of the victims [4] .

Some of the most common cybercrimes experienced by consumers today include debit/credit card fraud, hacking of an email or a social media account, electronic commerce frauds and disclosing private information to fraudsters via the telephone call or clicking on phishing emails [3]. Specifically, in the United Kingdom, it is estimated that the UK economy is suffering from the loss of around £27 billion per annum due to these cyber frauds [5]. UK businesses are affected the most at a cost of around £21 billion, followed by the government and citizens, with damage of around £3 billion each. The Internet Crime Complaint Center has received around 11,000 complaints in 2017, resulting in a loss of around $15 million, 90% higher than the losses reported in 2016 [6]. Furthermore, Microsoft also saw a substantial increase in the tech scam i.e. a 24% increase in tech scams reported by customers in 2017 over the previous year [7] with the average loss of $200 to $400 each. Fraud over financial systems such as ransomware, card payment, and Crime as a Service (CaaS) is found to be some of the established and professionalized ways to commit fraud [8].

In most cases, cybercriminals make use of customer facing platforms to target victims and practice cyber frauds [9, 10, 11]. Some of the highly targeted customer-facing platforms include but are not limited to: payment systems, where cybercriminals take control of the target victim's payment account, mobile platforms where a victim's mobile phone is targeted to get control over payment applications; and telecommunication systems where illegitimate acts are performed by targeting a victim through their telephony network. With the evolution in cyber systems, cybercriminals have also evolved in their methods of targeting cybersystems and there is a strong need to characterize the most used mechanisms of cyber crimes in order to protect organizations and consumers from cybercriminals.

In this paper, we discuss cybercrimes in three dimensions: 1) economics of cybercrime -- what is the cost of frauds and how much is required to have a defense, 2) attack mechanisms -- what attack mechanism criminals are using to defraud consumers and enterprises, and 3) prevention and detection systems -- what technical systems and techniques used by service providers to protect their consumers. We provided the economics of cyber crimes based on reports published by government agencies and security companies. We analyzed the fraud mechanisms in three diverse technologies: 1) card payment frauds, 2) mobile payment frauds and 3) telecommunication frauds. We choose these technologies for the following reasons: 1) the user base of these technologies is very large (e.g. there are around more than 5 billion telephone users), 2) collective frauds over these technologies are more than $60 billion [12, 13], 3) telephony has become the preferred media to target the user for payment and card frauds. The taxonomy of the attack vector of fraudsters in three networks is shown in Figure 1. We believe that this is the first study that covers various aspects of frauds on diverse technologies. Where applicable, the paper provides recommendations to improve the security of the system and safeguard individuals from the cybercriminals. This study would help consumers, regulators, service providers, and law enforcement agencies to know about how fraudsters are misusing the technologies and the defenses available to protect consumers.

In summary, the contributions of this paper are as follows:

- It provides a comprehensive survey of the economics of the frauds in broad areas of customer-facing technologies.
- It systematizes different types of frauds in card payment, mobile payment, and telephony, which all utilize the Internet technology for improving customer experience but in the meantime give rise a chance for cybercriminals to misuse the technology.
- It presents recommendations of best practices and technical countermeasures to address different types of frauds in these consumer-facing technologies.

This paper is organized as follows. Section 3 discusses credit card payment technologies, frauds over each method of card payments, attack mechanisms and possible defenses. Section

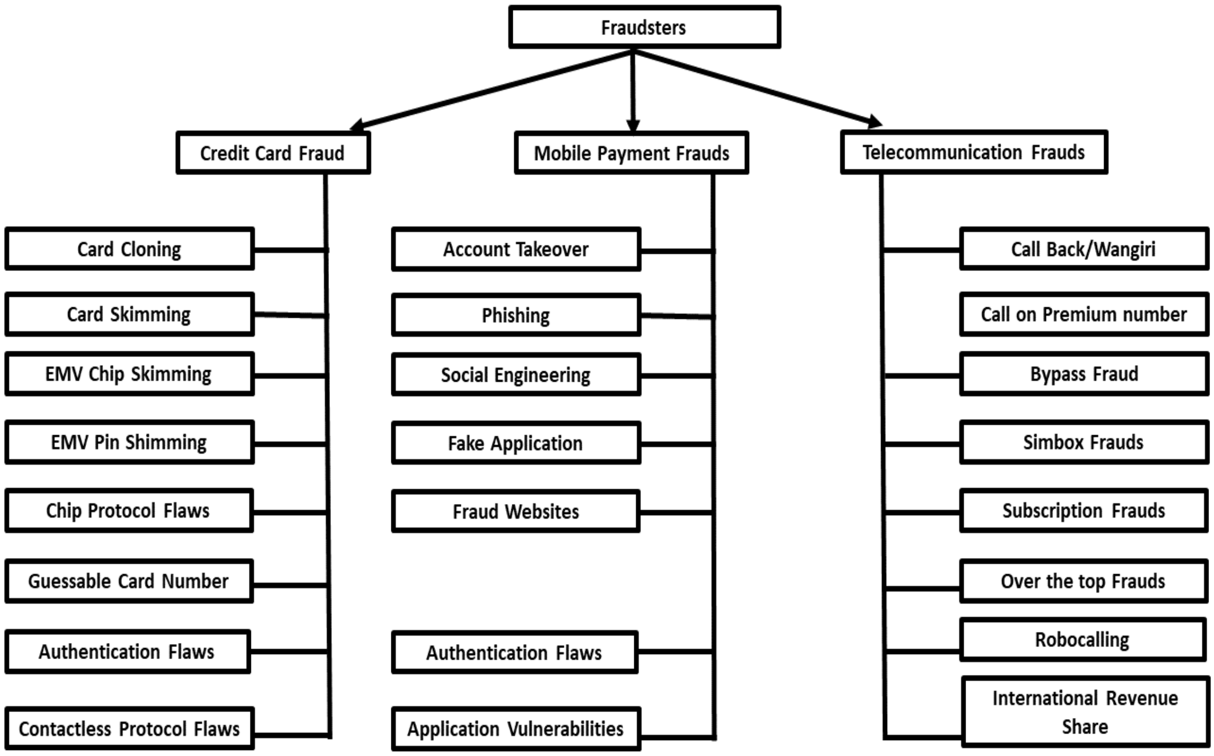

Figure 1: Taxonomy of Cybercriminals attack Vectors

4 presents discussions on frauds in mobile payment systems. Section 5 presents discussion on the frauds in telecommunication systems. Section 6 discusses ways forward and future directions to secure consumers from fraud. Section 7 concludes the paper.

2. Background definitions and Frauds over Internet Technologies

In this section we present background definitions based on [14, 15] and different types of frauds over the Internet technologies and e-commence systems.

2.1. Background Definitions

Cybercrime: The cybercrime can be defined as the computer and information technological offenses, which involve unauthorized access to user data, modification or impairment of electronic communications, using the user data for the personal benefits or financial gain. It also includes the distribution of unwanted content e.g. spam messages, illegal online content, such as child sexual abuse material, cyber-bullying, spreading the unwanted hatred and terrorism-related messages.

CyberCriminal: Any person who deliberately exploits vulnerabilities in computer or information systems in order to steal or compromise systems and networks for the misuse and malicious purpose.

Cyber fraud: Frauds that have been committed using the computer, mobile devices, and information technology systems such as hacking user devices and stealing the user's private information, phishing, and social engineering attacks, bypassing the billing system of the network providers etc. These frauds can have different shapes i.e. frauds against the payment systems, frauds against the technology providers and online frauds e.g. dating frauds, traveling frauds etc.

Cyber Defense: A proactive measure for preventing cyber intrusion, cyber attack, fraud attack, as well as determining the origin of operation in order to launch a preemptive, preventive, or cyber counter-operation against the source. It also includes ways to identify the attack mechanisms of cybercriminals.

2.2. Frauds Over Internet Technologies

Cybercriminals use the Internet technology for committing fraud activities in two ways: 1) spreading malicious content e.g malware, Trojans or viruses that in turn leak private information of the victims [16], and 2) convincing victims to disclose their private information via social engineering attacks. Internet-based applications have created new opportunities for businesses and retailers but at the same time, it has paved new ways for fraudsters to use the latest technology to commit fraud against users and businesses. Every year, a large number of people lose their money to different types of frauds over the Internet applications such as e-commerce, online dating, online gaming, credit card frauds, telephone frauds, mobile payment frauds etc. The e-commerce frauds can be of different type: e.g., the merchant does not deliver the product or has sent a product of lower quality than the advertisement. Some of the most common frauds happening today over the online marketplaces are buyers not receiving goods that they have ordered, receiving products that have inferior value or are significantly different from the original description [17]. The statistics by Experian show that e-commerce frauds (online auctions, buying products) have increased by 33% since 2015 [18]. Frauds over the online marketplaces have resulted in an annual loss of billions of dollars to customers all over the world [19, 20].

Over the Internet, fraudsters have created a large number of fake pages for two purposes: 1) they convince end-users to click on some links through social engineering or phishing attacks or exploit some browser system vulnerabilities to silently download malicious software on the user's computer whenever the user visits the malicious web page. These fraudsters also convince users to call a premium telephone number, which not only results in a financial loss but also disclosure of their financial information to fraudsters. Another type of fraud that is popular over the internet is Advanced Fee Fraud (AFF). This fraud is committed by asking victims to pay some amount to process their incentive, which can be in the form of leftover money of a deceased Nigerian rich person, an offer of a job with high pay, and the lucky win of being selected for a holiday vacation. The common attribute of these frauds is that the victim must pay a small amount of money first before they can get a bigger amount from the attacker later. The Internet of Things devices have also been used to target the end-users for the malicious activities [21, 22, 23, 24] e.g. DDos and massive spamming.

3. Card Payment Frauds

This section will provide an overview of card payment technologies and payment fraud as it affects the global payment system. We will start with a brief introduction to the payment system types. Section 3.1 discusses the card payments fraud landscape and details current fraud trends. Section 3.2 and Section 3.3 present an introduction to the technology and security features of each card payment type and will then detail the tools and techniques used by cybercriminals to abuse the card payment system.

Typically, a card payment system can be categorized into "card present" and "card not present" (CNP). In *card present* payment system, the cardholder is physically present at the merchant store and payment is performed by swiping (magnetic stripe), inserting (chip and PIN) or tapping (in case of contactless) a payment card to the merchant provided a point of sale (PoS) terminal/reader. With card present transactions the identity of the cardholder making a transaction is established either by requesting a card's PIN or by the cardholder signature. There are more security elements which when combined enhance the security of card present transactions. For example, the security features of a smart card with chip enables it to store payment related information securely. Card present payment security is further advanced with the use of cryptographic techniques that bind each transaction with a unique transaction specific code or cryptogram. Within card present payment technologies we have:

- Magnetic stripe cards
- EMV chip & PIN cards, with three protocol variants: Static Data Authentication (SDA), Dynamic Data Authentication (DDA) and Combined Data Authentication (CDA)
- EMV contactless cards, with three protocol variants (SDA, fast DDA, and fast CDA)

With *Card Not Present (CNP)* payment system, on the other hand, the cardholder enters her payment card details on the checkout page provided by the merchant website. The security of the CNP payment system relies upon the cardholder correctly providing her payment card details which may be shared with 'every' merchant that the cardholder makes a transaction with. A CNP payment system has two grievous security limitations. Firstly, the identity of the actual cardholder cannot be established by the merchant or by the card issuer and secondly, the card details are static and remain the same until the card service is expired. To overcome these limitations, the payment industry came with a user-authentication scheme which requires the cardholder to establish their identity with the card issuer before the transaction is approved.

We will expand more on the working and technology limitations of each type of the card payment systems in Section 2.1 to 2.5 but first, let us discuss the fraud landscape over card payments.

3.1. Economics of Card Payments Frauds

Payment card fraud is an international issue that spans across nations, states, and borders. Fraud from overpayment cards has amounted to a total of $22.80 billion globally in the year 2016 [25]. This is a 4.4% increase in the global card payment fraud rate as compared to the year 2015 where it was recorded $21.79 billion [25]. The United States (US) alone accounts for an overall of two-fifths (38.7%) of the global card payment fraud totaling to $8.45bn for the year 2016 and it is estimated that by the year 2020 the US card payment fraud could surpass $28bn [26]. To the contrary, card fraud losses for Europe in 2016 reached $2.12bn and about 73% of the European card fraud came from the United Kingdom (UK) and France [27]. In fact, for Europe, card payment fraud is one of the EMPACT priorities, under Europol's priority crime areas (2018-2021 EU Policy Cycle [28]). Over the last six years, it is established that the costs associated with the losses on financial systems constituted to the largest single category of fraud across the globe and over the Internet [27].

So how does a perpetrator succeed in practicing fraud over electronic payment systems? A simple answer to this question is that fraudsters in most cases target a weakness in the payment system technologies and exploit them for their interests and/or monetary gain. The methods used by fraudsters to abuse the payment system vary depending on the type of the system (among card present and CNP) being targeted. Fraudsters' methods can be well understood by mapping the payment card fraud patterns over the evolution/improvements of card payment technologies. For this study, we focus on payment card fraud patterns in the UK.

Figure 2 shows UK card fraud statistics[1] from 1998 to 2017 [29]. The statistics reveal that the ratio between the different types of card fraud changes year by year. In the figure 2, red, black and grey lines represent fraud losses on card present payment types and green line signifies the fraud that occurred over the CNP payment interface. Figure 2 also shows the introduction for significant security improvements in the card payment system technology listed below

1. Smartcards with EMV[2] Chip and Pin protocol: were introduced in 2004 replacing earlier magnetic stripe cards for card present transactions
2. Transaction risk profiling: card issuing banks started to use transaction risk profiling algorithms that assess the risks associated with transactions
3. More secure EMV protocol: the EMV protocol introduced a more secure form of transaction data authentication mitigating security flaws associated with earlier versions of EMV protocol implementations

Prior to 2004, before the introduction of EMV chip and pin, fraudsters had shown to target the magnetic stripe based card present transactions. CNP fraud, on the other hand,

[1]The UK was one of the early adopters of card payment technologies

[2]EMVCo [30] is a consortium of card payment networks (VisaCo, MasterCard, American Express, JCB and Discover) that was set up to maintain interoperability between payment card operations.

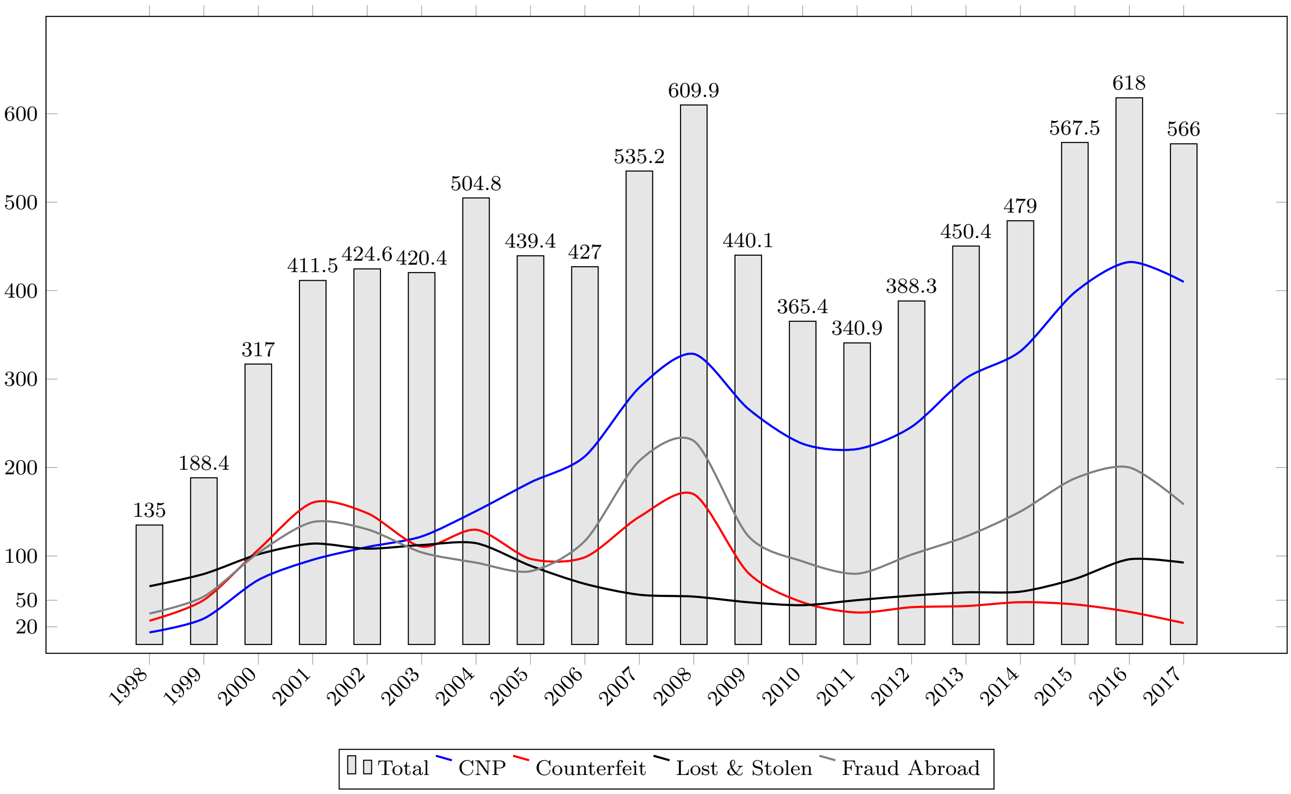

Figure 2: UK Card fraud by type from 1998 to 2017.

showed a gradual increase from the year 1997 to 2008 just before transaction risk profiling was introduced. However, fraudsters have shown to bypass CNP transaction safeguards as this is reflected by the growing fraud rates (from the year 2011) of CNP payment systems. CNP fraud stands out to be the single largest category of fraud amounting to a total of 70% of the total card fraud for the year 2016 [29].

Now that we understand the types and areas of fraud over card payment systems let us take a look at the technology behind each card payment system, security limitations of card payment systems and attacker methods which abuse the target payment system.

3.2. Magnetic Stripe Cards - Technology, Attacker Methods and Solutions

Magnetic stripe cards have a capability to store information which can be read electronically by a magnetic stripe reader. Each magnetic stripe payment card comes with a pre-loaded payment application that contains information about the user payment account as embedded by the card issuing bank. There are two tracks containing payment data located within the magnetic stripe Track 1 and Track 2. Track 1 includes all fields of Track 2 plus the cardholders name and additional fields for exclusive use by the card issuer. Mainly we have a field for 16-digit Primary Account Number (PAN) [3], cardholder name, cards expiry date, a service code which specifies the interchange rules and controls risk management functions and the final field is discretionary data which is used to provide security functions to a magnetic stripe transaction. Discretionary data include one or more of the following fields: PIN Verification Key Indicator (PKVI) [31] , PIN Verification Value (PVV) [31], Card Verification Value (CVV) [32] and Card Validation Code (CVC) [32]. With each magnetic stripe read, the card provides stored payment application data which is fetched by the PoS terminal to process a transaction. The terminal then applies security protocols for cardholder verification and risk management to complete a transaction.

Each magnetic stripe card has a cryptographically derived Card Verification Value (CVV) which makes magnetic stripe cards more secure than just having the PAN and expiry date [32]. CVV prevents counterfeit cards from being generated using the cardholder data obtained from paper receipts. CVV is a three-digit value generated by the card issuing banks and is embedded in card data before the card is issued to the cardholder. During a transaction, if there is a match in CVV received during the payment request to that of the locally generated CVV by the card issuer, the transaction data is marked to be authentic.

However, magnetic stripe cards work simply as memory sticks and are best suited for applications like ticketing, loyalty pass where security is not of prime importance. Apart from storing and retrieval of static data, not many operations could be performed on the magnetic stripe cards. The other problem associated with the magnetic stripe card is the amount of information that can be read. The access control policies on fetching the amount of data could not be defined on the magnetic stripe. This means any reader with a magnetic head can read all the contents stored on a magnetic stripe. This made possible for attackers to practice a trivial type of fraud on the magnetic stripe cards: *Skimming and Cloning.*

[3] A 16-digit card number which is also printed on the front of the card. PAN uniquely identifies the cardholder account with the card issuer

Figure 3: Showing a magnetic stripe skimming device found attached on an ATM machine [33]. The internal circuitry of the skimming device is also shown.

3.2.1. Magnetic Stripe Cards - Skimming and Card Cloning

In skimming fraud, the magnetic stripe technology cannot tell the difference between a real card and a counterfeit card generated through skimming shown in a Figure . In this type of fraud, ATMs are physically modified with minimal effort in a manner that is difficult for the cardholder to detect. The way skimming works is that thieves put a card scanner on top of the little slot where the payment card is typically inserted in an ATM machine. These skimmers allow the card to pass through them into the ATM slot while also scanning the card and stealing the numbers off it. This happens so discretely that many victims have no idea that something is amiss until they look at their bank statements probably weeks later. And because many ATM card slots use similar designs, there are plenty of skimmers that are designed to look almost exactly identical to legitimate card slots making it even harder for a customer to realize what is going on. Of course, though, the magnetic stripe transactions are protected with a PIN.To steal the PIN, miscreants also install small pinhole cameras in inconspicuous locations on the ATM to capture footage of the cardholder keying the PIN. To capture PIN, there are also number pad overlayers available on the black market which just look like the keypad on the ATM. Nowadays due to this becoming common practice, the public and banks have become more aware and the scammer may get caught when they try to retrieve their scamming equipment from the ATMs. To resolve this, more advanced skimming devices on the black market transmit stolen card information and PINs wirelessly making it much easier for the fraudsters to practice their scheme without getting caught. To overcome the magnetic stripe cards skimming and cloning attacks, the payment card industry introduced more secure forms of card payment which came in the form of EMV chip and PIN cards described next.

3.3. EMV Chip and PIN Cards - Technology, Attacker Methods, and Solutions

EMVCo created the "Integrated Circuit Card Specifications for Payment Systems"[34]. These specifications define an EMV chip and pin protocol [34], a messaging standard using which the payment cards operate and communicate with compatible readers. EMV utilizes features provided by the smart cards and supports either of the following three payment operations:

Static Data Authentication. SDA was only designed for initial versions of smart cards that had limited processing capability and can securely store only limited data. SDA validates the integrity of the application data stored within the smart card IC. However, SDA does not authenticate the card itself. During the card personalization phase (before the card is issued to the cardholder), the card issuer prepares the payment Application Data (AD) which is relevant to the cardholder account. The AD is signed with the card issuers private key (S1) and is stored in the smart card IC. The card issuer public key (P1) is signed by the Certificate Authoritys (CA's) private key (S_{CA}) and the issuer's public key certificate is stored in the smart card's memory. During the transaction process, when the cardholder inserts the card into the PoS terminal, the CA's public key (P_{CA}) (which is issued to the acquirer and resides with the PoS terminal) is used to verify the issuer public key certificate which resides within the card. The PoS terminal extracts the issuer public key (P1) from the certificate. In the next step, the PoS extracts the signed application data (signed by S1) from the card and validates it using P1. Once the signed application data is found valid, the reader and the issuer can be assured that the data in the smart card memory can be trusted and has not been altered.

Dynamic Data Authentication. DDA is an advanced scheme of card authentication, where each card is personalized with its private key used by the card to generate a signature Signed DDA (SDDA). The signature encodes transaction data and a random number given to the card by the PoS terminal which guarantees uniqueness for every transaction. In this scheme of card authentication, the cards public key (P_{IC}) is signed by the issuers private key (S1), and the card public key certificate is stored in the smart card IC. The issuer public key (P1) is further signed by CA's private key (S_{CA}), and issuer public key certificate is stored in the smart card IC. The CA's public keys are distributed to the PoS terminals. During the transaction, the validation of SDDA by the reader indicates that the card is authentic and is issued to the cardholder by the card issuer.

Combined Data Authentication. With CDA, both the PoS terminal and the card issuer verify the integrity of the payment card. Much similar to DDA, in CDA the card generates a transaction specific signature (SDDA) which is used by the PoS to verify the transaction. In addition, an Application Cryptogram (AC) is also generated by the issuing bank to be signed by the card using a shared secret key. An AC consists of transaction specific data and a random number which guarantees transaction uniqueness. During a transaction, a request to sign the AC is sent to the card by the card issuing bank. Having validated the received signed AC from the card, the issuing bank can guarantee the card authentication.

The above three EMV methods guarantee that the payment card is authentic and the data inside the card is unaltered by any adversary activity. The security of EMV enabled transaction is further enhanced with the use of card's PIN only known to a valid cardholder. This guarantees that only the authorized person entitled by the card issuing bank is using the card. These security features make EMV the most suitable payment protocol for card payments. On the flip side, EMV payment cards also exhibit certain limitations which affect the security of other forms of the payment system. Below we will discuss limitations or attacks that were exploited on the EMV chip and pin payment cards.

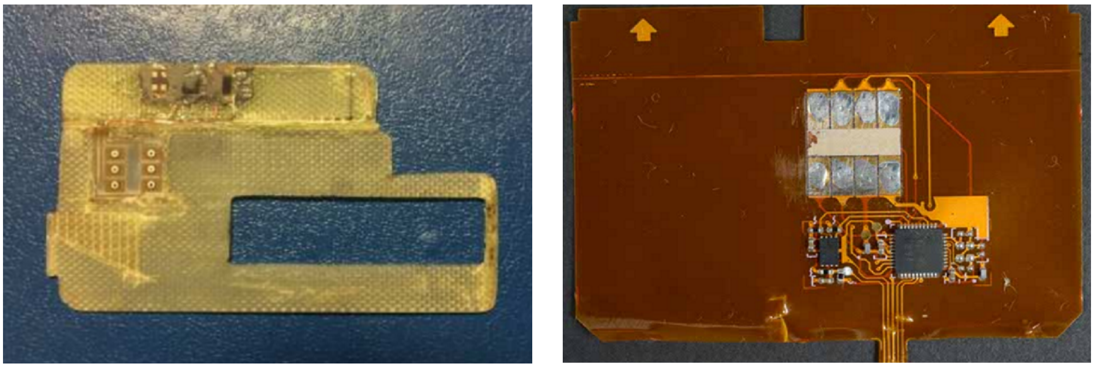

Figure 4: Shows two EMV shimmer devices found in EMV enabled ATM machines. On the left, it is a shimmer device found in Canada and on the right side one was discovered in an ATM machine in Europe. Figures of shimmer devices are taken from [35].

3.3.1. EMV Chip and Pin Shimming

As discussed in the previous section, EMV defines functions that establish the authenticity of the card, however, there is no mechanism defined which verifies the authenticity of the reader that the card communicates with. This provides ample opportunity for an attacker with a rogue reader to communicate with the EMV card. Figure 4 shows two EMV shimmer devices found in EMV enabled ATM machines. These shimmers are attacker tools that intercept communication between the EMV card and a PoS terminal or an ATM. Although there is no known possibility for an attacker to create a cloned copy of the victim's EMV card, the shimmed details can be used to create a magnetic stripe version of the victim's card.

EMV smart card chip contains all components of cardholder payment application data found in the magnetic stripe except CVV. The EMV interface contains its own version of Card Verification Value generally referred to as iCVV or dynamic CVV. iCVV which is different from magnetic stripe CVV prevents the shimmed data being copied and used over magnetic stripe interface. The rationality behind the success of skimming can be related to the negligence of some card issuing banks while validating the CVV. Skimming works because some card issuing banks do not validate the CVV while authorizing a magnetic stripe transaction [35].

3.3.2. EMV Chip and PIN Protocol Flaws

EMV Chip and Pin is an open-source and well-documented protocol. The proven complexity of the EMV Chip and Pin protocol and its widespread use across the globe has made the protocol much attractive for research communities. There is a substantial amount of research addressing the security analysis of the EMV Chip and Pin protocol. We will focus on one research activity which has identified a practical exploitable vulnerability in the EMV protocol.

Murdoch et al. (2010) [36] identified a flaw in the EMV chip and pin protocol which allows an attacker to authorize a payment while entering an incorrect PIN. Researchers introduced a man-in-the-middle device which can subvert the cardholder verification process by telling the PoS terminal that the PIN entered by the attacker is correct, whilst telling the EMV card that this is a transaction verified by signature and therefore no PIN is required. This bypass the primary security of the EMV Chip & PIN protocol, i.e. the cardholder PIN. The research team performed practical experiments to demonstrate that the vulnerability was present in the UK issued credit/debit cards and UK PoS terminals. The importance of this research was highlighted in the year 2012 when fraudsters were arrested in France. It was discovered that the fraudsters had exploited this vulnerability to conduct 6,000 fraudulent purchases with a total value of more than €500,000 [37].

3.4. EMV Contactless: Technology, Attacker Methods and Solutions

The advancements in the EMV payment ecosystem towards fast and secure payments were announced with the introduction of contactless cards. Unlike chip and PIN cards which require a point of contact for communication with the reader, a contactless card talks to the PoS terminal wirelessly using the RFID technology. Contactless payments are designed for low-cost in-store payments usually about £30 in the UK and do not require PIN verification for cardholder authentication.

The EMV contactless transaction protocol [38] is derived from the EMV chip and pin protocol and is further enhanced to minimize the transaction processing times at the PoS terminal. The EMV contactless specifications define at least two variants of the contactless transaction protocol. Both of these protocol sequences derive three security features from the EMV chip and pin protocol as defined in Section 3.3. Although proven to provide convenience to the customer and speed to the low-value payments, the contactless interface of EMV payment cards has introduced a new series of attack vectors on card payments which are discussed below:

3.4.1. EMV Contactless Protocol Flaws

Emms et al. (2013) [39] exploited the EMV offline Pin verify command from the contactless interface. Contactless transactions do not require the cardholder to enter their PIN. However, the researchers discovered the offline PIN verify command is functionally available on most of the UK issued payment cards. This PIN verifies command can be exploited by an attacker to guess the card PIN without blocking the card. The research demonstrated a viable attack scenario where a contactless physical access control reader is programmed with part of an EMV transaction protocol. When the user scans a wallet with the payment card onto the access control reader, it selects a payment application on the card.

In another study, Emms et al. (2014) [40] exploited a currency limit handling command in the EMV contactless specifications. Typically, for UK based payments cards the maximum threshold for a transaction value is £30. However, the researchers demonstrated that for contactless cards, when a transaction is made in a currency type foreign to the card issuer's country, the card will allow transactions of unlimited value.

3.5. CNP Payments - Technology, Limitations and Attacker Methods

The ease and convenience with which a customer can make purchases over the Internet benefited both the customer and the merchants alike. Within the CNP payment system we have *authorization-only* and *user-authentication* enabled CNP payment protocols.

Authorization-only CNP protocols provided more convenience to the shopping process where customers were only required to fill and submit their payment card details which include 16 digit card number, card's expiry date, three-digit card security code (CVV2) and cardholder address information to the Internet-based merchants. For fraudsters, however, this convenience came as an opportunity to steal customer's card details and misuse them.

The first attempt to combat growing CNP payment fraud came in the year 2001 where payment networks (Visa, MasterCard, American Express et al.) introduced the 3 Domain Secure (3DS) protocol. It introduced the concept of user-authentication for payment transactions over the Internet. For every CNP payment transaction, 3DS required the customers to provide a password, thus combating the growing CNP payment fraud. However, the 3DS protocol exhibited two design flaws: activation during shopping and the use of static passwords. Activation during shopping required the cardholders to register with 3DS during the time of purchase. This enabled even attackers with stolen card details to register the victim's card over the 3DS. Additionally, attackers were still able to trick victims to give away their static 3DS password. Because of these reasons most merchants still stay hesitant to adopt the 3DS and prefer using the authorization-only CNP payment protocol. This freedom of choice for the merchants (i.e. the use of user authentication and/or authorization-only), in the ways to accept online payments, even left pathways for the attacker to exploit loopholes and practice fraud over the CNP payment system.

The most common techniques employed by fraudsters to abuse the CNP payment include *phishing* and targeting the victim's machines with specially crafted *malware* which is designed to steal payment card details. Stolen card details are either used by adversaries or are traded on online portals. Trading of credit card numbers in the underground market has previously been studied in the academic literature [41, 42]. Even today the trading of credit card details remains active as we provide a list of at least 15 live illicit websites/forums [See Table A.4 in Appendix A] where card details are still traded. Since phishing [43][44], card details stealing malware[45][46][47] and trading of card details in underground forums [48][49] have been comprehensively studied, we do not expand these attacker techniques in this paper. In the following sections we detail three limitations that we explored within the CNP payment system:

- Card Skimming (Magstripe, EMV Chip and PIN and EMV Contactless)
- Merchant Receipts and Guessable Card Numbers
- Architecture of Authorization Response Codes

3.5.1. Card skimming

Also as discussed in Section 3.3.2 the design of card present payment protocols [34][50][51] mandates the card number to be stored as plain text within the cards memory; this enables even an illegitimate card reader to communicate and interpret the card details. Such an unusual design for a payment protocol offers at least two opportunities for an attacker to obtain payment card details. Firstly, it is well-known for a contactless card that card number and expiry date could be skimmed from a distance with any NFC enabled device [33][52]

Figure 5: Merchant receipts exploiting full payment card number and expiry date in plain text.

Table 2: Card number information fields (Numbering is from left to right)

Card number: 4658 - 5900 - 0000 - 000C
First six digits: called as Bank Identification Number (BIN), identifies the card brand and issuing bank
Digits 7 to (15): assigned by the card issuing bank and denotes personal account number shown as zeroś
Last digit: akin to checksum (indicated by 'C'), used by a computer to verify the card number entered is correct

and in fact, in a single Google play search, we located 38 freely available Android apps which could be used by an attacker to read the contactless payment cards. Another channel that an adversary can follow to obtain the card number details is from the merchants sales receipt printed from the Point of Sale (POS) terminal.

3.5.2. Merchant Receipts and Guessable Card Numbers

To maintain sales records made using payment cards, in-store merchants maintain a merchant copy of the customers transaction. We found that merchant copies from a number of high street retailers revealed their customer's complete payment card number and expiry date (shown in Figure 5). These card details are enough to create transactions and purchase goods from giant online merchants stores like Amazon [33]. Worst of all, none of the merchants were educated about the risks of losing merchant copies, and a few of the merchants even agreed to sell several merchant copies for under a dollar. This means, whenever a customer uses their card with in-store retailers, there is a risk of having the card number stolen. Just from around our organization, we found 23 such retailers whose merchant copy revealed the full card number and expiry date.

We further investigated the possibility of an attacker generating payment card numbers and explored that an adversary could easily produce and validate a database of active

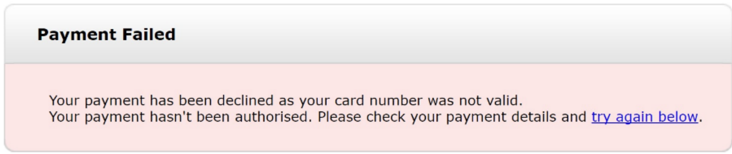

Figure 6: Response code revealing the validity of a card number

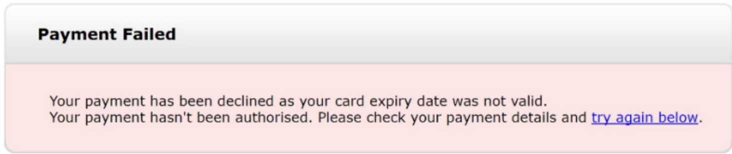

Figure 7: Response code revealing the validity of a card number and expiry date

payment card numbers as discussed below:

The payment card numbering specifications are governed by the ISO/IEC 7812-1:2017 [53] and the ISO 10202-6:1994 [54]. Table 2 enumerates the useful insights that can be obtained from a credit card number. It can be learned from a card number that customer account number fills nine spaces and therefore, the maximum number of possible active card numbers for a bank would be one less to 10^9 (a billion). An attacker starts by selecting the target banks BIN (the bank with a high number of customers would give high positives), randomly generates thousands of accounts number using Luhn's check algorithm [55] (or with automated bots as demonstrated in [52]) and makes transactions using the generated card numbers on online payment websites. When a transaction is made, a transaction authorization request is sent by the merchant to the card issuing bank. The card issuing bank, through authorization response message (further discussed in the next section), indicates to the merchant that the card number used while trying to make a purchase is not correct. For an attacker, the authorization response will reveal the validity of a card number.

For example, when we made a transaction with an invalid card number on a merchant website-x (website name masked), we received the response as shown in Figure 6. If the card number was valid, the authorization only changes to indicate any other invalid card data element (as shown in Figure 7). A recent investigation into Tesco bank breach revealed that attackers used a similar technique to exploit payment card details of around 9000 customers [56]. Additionally, we observed a weak security practice by a leading card issuer (name masked) when they issued payment card numbers to their customers. We found that the card issuer issued payment card numbers in a serial guessable sequence. Shown in Figure 8 are three payment cards belonging to the same customer and card numbers are shown issued in a sequence with a difference of 8.

3.5.3. Architecture of Authorization Response Codes

As discussed, after a merchant submits an authorization request (AuthzReq), the cardholder bank responds to the merchant or its payment processor with what is known as an authorization response (AuthzRes). The AuthzRes is a string of complex codes which indi-

Figure 8: Payment cards belonging to the same customer and card numbers are shown issued in a sequence

Table 3: Authorization response code for merchant with PayPal as payment processor

`RESULT =114& PNREF =VXYZ01234567& RESPMSG =114 & AVSADDR=N & AVSZIP =N& IAVS =N& CVV2MATCH =N`

RESULT	> 0	Result > 0 indicates the transaction was declined. RESPMSG gives a brief reason for the decline of the transaction
PNREF	Value	A unique value that identifies a transaction
RESPMSG	114	The transaction was declined (Card security code doesn't match). RESPMSG 114 implies that the transaction was declined because of the invalid CVV2
AVSADDR	N	Address of the card holder was not verified for the transaction
AVSZIP	N	Postcode provided at the checkout matches with card holder's bank file
IAV	N	Cardholder country code is local
CVV2MATCH	N	Card security code mismatch

cates to the merchant the transaction status and any card data field put incorrectly by the cardholder. To make AuthzRes codes readable to the customers at checkout, these response codes are parsed by the merchants into the user understandable language. These codes could be used to learn all card data fields.

Table 3 shows an AuthzRes code for the merchant with PayPal as its payment processor. It can be derived from Table 3 that the transaction was declined because CVV2 supplied at checkout by the customer does not match with the actual cardholder file with the bank's authorization server. This AuthRes code also implies that the card number and the expiry date were valid. In the next step, the AuthRes code is simplified at the checkout in user natural language. For example, during our experiments, with valid card numbers when the expiry was not entered correctly while making a purchase on website x (name masked), the parsed response string as shown in Figure 7 explicitly stated "Your payment has been declined as your card expiry date was not valid". Having known that the VISA authorization network does not detect multiple invalid attempts when distributed across multiple payment gateways [52], an attacker has countless attempts to guess expiry date and all the other card data required to make an online payment [52]. Using the AuthRes codes an attacker could easily be able to obtain card data fields for all Visa cards [52].

4. Mobile Payment Frauds

Over the years, mobile devices such as smartphones and tablets have started to replace desktop computers. Fraudsters have caught the wave of opportunity and they have been shifting their activities to this channel [57]. Mobile web fraud strategies are quite similar to those used on traditional online fraud, making the adaptation of cyber frauds to the mobile situation often straightforward. Furthermore, fraudsters have found new chances to make a profit specifically for mobile applications.

Some of the characteristics that have helped to increase the popularity of mobile devices such as ease of use and mobility, create new security risks not associated with computers. It is common that mobile devices are often shared with friends and family, and it is potentially easier to leave them unattended in public spaces where they can be used for a second person or easily stolen.

Mobile payments have been adopted in different ways. We are using mobile devices for online shopping and to pay for digital services. Moreover, they have become popular for contactless payments instead of paying with debit or credit cards. The main models for mobile payments usually are relayed in one of the following technologies [58]:

- Stored value account systems: Usually the method is integrated into an app on the mobile device i.e. payment wallet. Apple Pay, Samsung Pay, Android Pay, Microsoft Wallet, and PayPal are the most widely used wallets, with Paypal being the only one which works across different operating systems. They allow a customer to make faster online payments (when the merchant accept them) and contactless transactions using the Near Field Communication technology included in many mobile devices. Other popular wallet apps are brand specific, such as Boost Mobile and the Starbucks Wallet app which usually include loyalty programs.

- Account based systems: A mobile web payment system can store card details which can be remembered for future purchases turning the payment into a simple click-to-buy. Commonly, strong authentication is required to commit large value payments. Banks have taken advantage of this technology and they have developed applications which allow customers to operate in their accounts in real-time i.e. direct transfers.

- Mobile billing systems: The customer uses a premium SMS or direct carrier billing during the checkout. The success of earlier mobile content services such as logos and ringtones accustomed consumers to using this type of payment. An advantage of this type of payment is that existing telecom operator billing systems are suitable for handling micropayments transactions.

A common way to steal payment information is through malware which has been installed previously in the device. Other ways are social engineering and fake apps [59, 60, 61]. Because of the low prices of mobile devices, fraudsters can afford using many different devices to commit the attack and most of the observed fraudulent e-commerce transactions are originated from new devices[62]. Using new devices, fraudsters can avoid some of the traditional anti-fraud measures such as those based on a persistent identification which i.e. the merchant can identify that is the same device trying to get access to a different account.

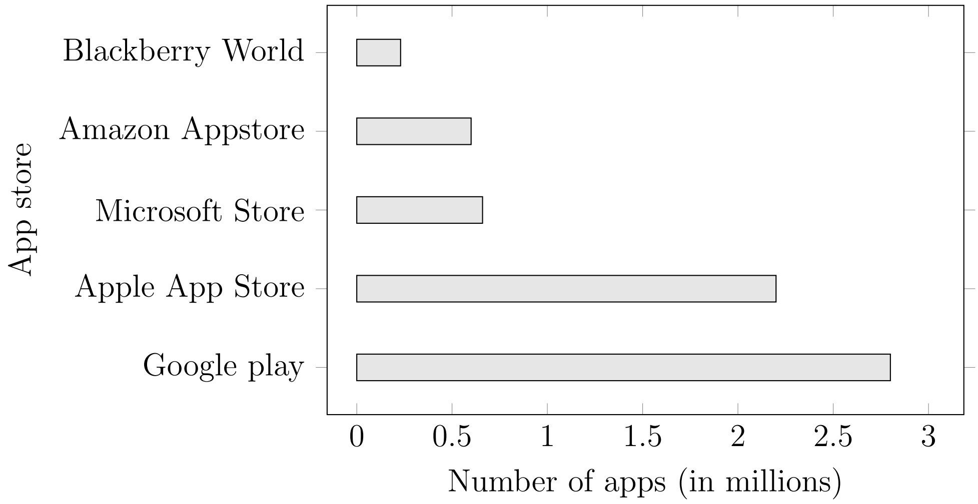

Figure 9: Number of apps available in leading app stores in first quarter of 2018.

4.1. Economics of Mobile Payment Fraud

During the first quarter of 2018 more than half of the financial transactions took place on mobile devices [62] and it has been on this mobile platform where the highest percentage of fraudulent operations have taken place. However, the awareness of risks for mobile payments is low and many merchants believe that mobile devices are more secure than computers [63].

On the other hand, the number of merchants offering their services through apps instead through dedicated mobile websites has grown considerably, especially for merchants with high revenue [64]. At the end of the first quarter of 2018, there were 7.1 million mobile applications available at the leading app stores of the market [65] (Figure 9 shows the number of applications available by most popular app stores in this period). At the same time, the proportion of cyber fraud carried out using mobile apps has increased from 5% to 39% in the last three years [66].

4.2. Attack Methods in Mobile Payments

Many types of fraud affect the end-user of mobile devices. We describe the group with a higher incidence.

4.2.1. Account Takeover

Account takeover is the most frequent type of fraud [67]. After fraudsters have found out about the access information of a user, they utilize it to sign up for an expensive service or purchase a product. Bad actors manage to access personally identifiable information in many different ways such as data breaches which become more and more frequent i.e. between May and July of 2017, Equifax, one of the largest credit bureaus in the U.S, was a victim of a data breach. In this case, personal information of almost 150 million of customers was exposed, including in a few cases credit card data [68].

Once an account has been taken over, it is difficult to fight because both legitimate and fraudulent users use the correct login credentials. Customers are particularly vulnerable when they do not use strong passwords and they re-use them for several accounts [69]. Especially when the provider utilizes a one-factor authentication method that increases the exposure of the users. For example, after the coffee chain Starbucks launched an app which allowed customers to pay for their coffee, several customers reported that money was withdrawn from their accounts without authorization [70]. After fraudsters managed to log into the app, they top up the account using the stored credit card and then they purchased gift cards which can be sold in the black market. The company said that criminals were obtaining login credentials from hacked websites and trying them out in the Starbucks app.

4.2.2. Phishing

Phishing is a well-known cyber attack where fraudsters steal personal information from users under false pretense by email, phone call or social media sites. It is one of the oldest types of cyber fraud attacks but still it is frequently used in mobile channels i.e. mobile users are 18 times more likely to be exposed to a phishing attempt than to malware [71], and three times more vulnerable to a phishing attack than to computers [72]. While many users have learned to be suspicious of links and attachments in emails, however, today 66% of emails are checked on the mobile devices [73]. Similarly, the popularity of mobile applications like SMS and WhatsApp also attracted the fraudsters to utilize the medium for getting personal information of the victim via the phishing attack.

4.2.3. Fake Applications

Scammers develop fake apps which may include malware or be designed to steal personal info. Sometimes phantom applications use an organization brand without permission to easily trick the user. Financial Trojan horse malware is one of the most popular cases because of the increasing availability of malware-as-a-service kits available in the cyber underground [62]. In some cases, the fake application sends premium SMS messages where an amount of money charged to the phone bill of the user goes directly to the fraudsters. Several researchers demonstrated the use of fake Near Field Communication (NFC) reader application on android enabled platforms. NFC enabled mobile phones to use ISO 14443 Identification cards – Contactless integrated circuit cards – Proximity cards (part 1-4) communication standards and these are the same standards as used by contactless payment cards and readers to facilitate payments.

Mehrnezad et al. in [74] demonstrated the practicality of fake NFC applications initiating a fraudulent transaction with contactless payment cards. In that, the researchers were able to design a fake NFC app on an Android phone which can interact with the contactless cards kept in a mobile phone wallet and make fraudulent transactions, read user locations and upload these to an attacker-controlled server. In fact, in a single Google play search, we found 38 such NFC android mobile applications capable of reading contactless payment cards.

4.2.4. Fraudulent Website

A large number of fake websites will use a domain name that impersonates or refer to a well-known brand. But this would not represent the official website. For example, you apply for the job online, and they ask to deposit funds to process your application. This type of fraud shows the same characteristics of the computer case. However, in mobile devices, it is more successful because users are less likely to notice that a website is slightly different than the original [75]. This is because, screens size of mobile devices are relatively small, constraining the user interface. This makes it considerably more difficult for users to recognize which mobile application or website they are interacting with [76].

4.3. Systems for Detecting Frauds In Mobile Payment Systems

The trade-off of usability-security is the main concern when implementing anti-fraud measures. Users do not want their online experience to be affected by security steps. At the same time, merchants know that if they are not able to provide a smooth setting, they will have to deal with the user disappointment and economic loss.

On the other hand, because of the specific hardware specifications of mobile devices, the adopted measures must meet certain intrinsic aspects of the platform:

- lightweight: computational demand of the system has to be low since mobile computational power is limited.
- restrict the communications: some mobile device users i.e. smartphone users, can be charged by data rates. Additionally, bandwidth or data usage may be limited. Therefore, the amount of information sent and received for the security approach should be low.
- restrict energy consumption: battery life is nowadays a big concern in mobile technology. It is required that the energy consumption level is as much efficient as possible.

4.3.1. Control access: authentication mechanisms

Because of the friendly portability of mobile devices, access control measures are necessary. An authentication mechanism is a common measure to prevent unauthorized access to the device. In an authentication process, the identity of the user is verified according to the information provided either directly or indirectly by the user. We can classify authentication methods to the following:

- Knowledge-based methods: the process is based on information which the user knows i.e. a password or a Personal Identification Number (PIN).
- Object-based methods: the process is based on something the user possesses i.e. a hardware token.
- Biometric-based methods: the process is based on information obtained usually from sensors. This information describes the physical or behavioral characteristics of the users such as the tone, cadence, and pitch of their voice.

In [77] researchers introduced an object-based approach using a Bluetooth token. In this approach, when the user attempts to gain access to the device, a smartphone tries to communicate with a token through Bluetooth connection. If the token can be reached and the smartphone receives confirmation of the communication, it will be unlocked. However, object-based authentication methods have been rarely implemented for mobile devices. Nowadays, people bring their devices most of the time with them, and the obligation to carry on an authentication device makes these systems less practical.

Knowledge-based methods have been used for a long time on mobile authentication processes and they are still used widely. PIN and password have been for years the most common authentication approach, despite that their inconvenience and weakness have been proved many times. This method is susceptible to simple attacks i.e. shoulder surfing where fraudsters spy the actions of victims and smudge attacks where smudge stains on the display are used to infer the password [78]. On the other hand, because the user has to remember the code, often they either use the same memorable instance for different accounts or they choose a weak one. A study has shown that among over $6,000,000$ passwords, 91% of all of them belong to a list of just $1,000$. The same study points out that in this list 8.5% of the individuals use either password or 123456 as a password [79]. Furthermore, passwords have been reported stolen from big databases on many occasions.

Some approaches have tried to overcome some of the limitations of PINs and passwords. In [80], researchers introduce a graphical authentication system which attempts to confuse an observer with different information each time the user tries to log in. In order to make the system more manageable, users have to remember a group of images instead of codes and they will have to select the images they know among those revealed. The study showed an increment of the time to log in and lower success rate. In [78] the researchers attempted to address the threat of the shoulder surfing attack. In this case, the user should draw a shape in the back of the device, the area which should be more difficult for someone over the shoulder to watch. The system was developed in a prototype because the additional hardware required is not available in any smartphone in the market.

However, PIN/Passwords are intrusive techniques which require a specific action of the user and they take place only once at the beginning of the session.

Biometrics based methods have been introduced more recently and they are receiving a lot of attention from the community. Biometric data describe the physical or behavioral characteristics of a human being. Different sources will include different attributes such as features which describe a voice pattern and motion patterns.

A Biometric Authentication System (BAS) evaluates biometric data for verification or identification of individuals. Nowadays, many different sensors have been incorporated in the smartphone such as environmental, location and motion sensors. Obtaining biometric data from them is easy and straightforward and BAS have been used in many practical applications successfully.

With the integration of low-cost and high-quality cameras on mobile devices, face recognition authentication methods, which had been used widely in banking and security access systems, become popular for unlocking the mobile devices [81] [82]. In a face recognition approach, the system stores patterns of feature images or video frames which characterized the user i.e. relative position, size, and shape of the eyes. One of the main threats of this method is the spoofing attack. In the simplest face spoofing attacks such as print attacks and replay attacks, the scammer basically tries to mislead the system by showing to the camera an image of the victim. Nowadays, with the popularity of social networks, it is very easy to have access to photos and videos from most of people. More sophisticated attacks i.e. the 3D Masks attack, use a 3d-scanners. Measures to improve these methods have been proposed for both but results are still limited [83]. An additional concern in this approaches is that the process of face capturing is influenced by a lot of external conditions such as the illumination in the scenario and the clothes worn by the individual.

As same as face recognition, iris recognition uses the devices camera to capture biometric features. Most of the non-mobile iris authentication systems use images taken in near-infrared illumination because, at the infrared spectrum, the finest textural patterns of an iris are revealed [84]. Quality of the camera on mobile devices has improved drastically, but few operate in the near-infrared spectrum. Furthermore, when a picture of the iris is taken in real scenarios, distortion is introduced because effects such as low light, shadow, and off-angle gaze direction, decreases the accuracy of the method [85].

Periocular authentication systems share a lot of similarities with iris and face recognition schemes. Periocular biometric features are extracted from an image of the facial region in the vicinity of the eye. The main advantage compared to the iris recognition method is the easier way to capture the image. Furthermore, invisible (near infrared) lighting is not required to capture the image. Extensive research of this method for authentication has been done on smartphone platforms [86].

More recently, some manufacturers have included a fingerprint reader in their devices to authenticate users [87]. This method has a lot of similarities to face recognition. The main difference is that the features used to discriminate between users are those obtained from print patterns of the individual. Many users trust this authentication method [88]. However, this method usually is not very accurate [89]. Conventional touch sensors introduce physical distortion because of the pressure applied by the individual which critically affects the authentication process. Furthermore, the classification is influenced for other environmental factors such as humidity. Finally, fingerprint images of databases represent a huge risk. There have been multiple cases where information from password databases has been stolen. When information from a fingerprint database was stolen, authentication patterns could not be reset.

Voice recognition authentication methods are based on the idea that the voice of each individual has unique characteristics that can help distinguish between users. Banks have been very interested in this technology because they could be integrated into telephone banking applications. However, a study which compares the usability of several biometric authentication methods found voice recognition less user-friendly than password entry and face recognition [90]. In the mentioned study, most of the participants involved gave negative feedback about the method.

Another biometric authentication approach which has been extensively studied on mobile devices is touchscreen recognition. This method is based on the idea that the manner that the user touch the screen can be used to authenticate individuals. Usually, this method is applied in continuous approaches i.e. the user is authenticated continuously during the whole session with a certain frequency which depends on the capabilities of the system. The obvious limitation of this approach for continuous authentication is that not all the activities involve touch actions.

Continuous authentication approaches are non-intrusive. With the inclusion of motion sensors such as the accelerometer, the magnetometer, and the gyroscope, motion authentication for mobile devices has become more popular. Usually, motion recognition is used on continuous authentication approaches too. Some studies have been focused on identifying users based in the way they walk [91] and in the way the hold the device [92, 93].

A biometric multimodal approach is based on data from several sensors. For example, in [94] the authors proposed a method combining three authentication techniques i.e. face, iris, and periocular recognition. In this system, information was extracted from the same image previously taken from the devices camera. The authors calculated a fused similarity score based on the individual score of each recognition method. They tested four different fusion rules, obtaining the best performance of an EER of 0.68% with a Dynamic Weighted-score procedure.

4.3.2. Machine Learning to fight Payment Frauds

The industry is continually seeking measures to combat fraud activities. However, where a new protective procedure is introduced fraudsters adapt to it.

Because of the low prices of mobile devices, fraudsters can afford using many different devices to commit the attack and most of the observed fraudulent e-commerce transactions are originated from devices that are 'new' [62]. Operating in this manner, fraudsters can avoid some of the traditional anti-fraud measures such as those based on persistent identification.

As we have mentioned, one step authentication processes are easier to hijack especially because users many times utilize the same access info for different services. Combining several types of measures makes the device less likely to be compromised. In this scene, Machine Learning (ML) techniques begin to play an important role. The use of ML in identifying and mitigating fraud has grown 13% since 2015 [64]. ML algorithms are employed to analyze behavioral data related to the users, helping to detect anomaly patterns which can be correlated with fraud. ML algorithms have proved to be very efficient, but their use of mobile devices is limited to the computational resources available. For this reason, some authors propose a distributed approach in which some of the computational burdens are offloaded to the cloud [95].

Supervised techniques such as Support Vector Machine (SVM) and Hidden Markov Model (HMM) [96, 97] have been actively studied. In [91] the authors compared both techniques to identify users based on the way they walk. The authors showed that SVM was slightly superior to HMM with an Equal Error Rate (EER) of around 10%. In the same context, researchers in [98] showed that the K-Nearest Neighbours technique achieved slightly better results than HMM and SVM. These techniques as well have been studied in other contexts such as touch recognition [99, 100, 101], use of the software [102] and malware detection [103, 104, 105].

On supervised approaches, the model is trained with normal and fraudulent samples which limit the operation of the system when the fraudulent patterns change. One-class SVM is a semi-supervised algorithm that learns a decision function to classify new data as similar or different to the training set which only includes normal samples. In [106] the authors introduced a multi-modal approach which employed accelerometer and gyroscope data together with touch biometrics. First, the authors use a one-class SVM model to classify the samples as either belonging to the owner or another person. The decision is made based on a group of samples instead of a single observation. Subsequently, they build a dataset based on the previous classification process to train a two-class SVM. With some similarities, more recently a semi-supervised approach was proposed [107]. The authors use the same sources of data and a classification algorithm based on the one-class SVM method. They test the approach with a dataset collected in a controlled environment where users were asked to type text during sitting and walking. They obtained an EER of 7.16% when the user was walking and 10.05% when the user was sitting. The authors deferred the evaluation of the approach on real-world scenarios to future studies.

More recently, other semi-supervised approaches have been proposed based in Deep Learning techniques such as Convolutional and Recurrent Neural Networks. In [93, 92] the authors used a CNN to identify smartphone users in the way they hold the device.

5. Telecommunication Frauds

The telephone system has become an integral part of the daily routine. There are more than 6 billion telephony users across the world [108, 109]. The huge customer base, easy integration with the Internet and cheap call rate have made telephone network a lucrative medium for fraudsters to target victims in real-time. In this section, first, we provide economics of telecommunication frauds, then provide the methods which fraudsters are using to target the victim and then present brief discussions on methods designed to protect the network and consumers.

5.1. Economics of Telecommunication Frauds

Telecommunication systems (Mobile, Fixed, Internet Telephony) have become an integral of humans life by staying in touch with friends and family and doing business communications. As of 2017, the number of telecommunication users in the United Kingdom is approximately 125.5 million (Fixed and Mobile). The rapid increase of the user base and the cheap telephony rate over the Internet Telephony (VoIP (Voice over IP)) have also facilitated scammers and fraudsters to use this medium for financial benefits. Scammers over the Internet telephony can use spoofed identities of the legitimate entities (for example banks, tax department) or use non-traceable anonymous identities for making unsolicited calls and messages to the telephony users. These calls and messages not only annoy call receivers with the unwanted ringing but would also result in a financial loss.

There are around $2.25 trillion accumulated losses in the telecommunication industry across the globe as reported by the Communications Fraud Control Association (CFCA) [13]. It is estimated that unsolicited or spam calls over telephony results in a loss of $38.1 billion per year to the fraudsters and scammers. This is 1.69% of the total telecommunication revenue. Moreover, FTC (Federal Trade Communication) has estimated that people in the USA lose $8.6 billion annually to the fraudsters, and the majority of fraudsters use telephony medium for the purpose. The following are the top categories of frauds in the telecommunication networks: \$0.8 billion to SMS Faking or Spoofing, \$1.6 billion to Phishing and Pharming, \$1.8 billion to Wangiri (Call Back attack) [13].

5.2. Attack Methods in Telecommunication Frauds

This section list some of the most common fraud types and their attack mechanism.

5.2.1. Wangiri Fraud

Wangiri (literally, “ring and disconnect”) is a type of fraud call that was first originated in Japan back in 2002 [110]. In the wangiri call attack, the attacker convinces call recipients to call at a premium rate a national or international phone number. The attacker made a short miscall on the victim phone and curious recipients assume that they have missed a call from the legitimate caller and call back the number. They are then charged at the premium call rate for this call. The user does not realize they are a victim of this fraud until they receive the monthly bill from the service provider. In this attack, the attacker convinces the callee to callback on the premium number which is under the control of fraudsters.

5.2.2. Simbox or ByPass Fraud

Bypass Fraud or SIM Box fraud is the most costly type of fraud affecting the regulator as well as the telecommunication service provider. The Bypass fraud is common in regions or countries where call rates for international termination are substantially higher than the local landline or mobile call charges. The fraud results in an average annual loss of \$ 4.3 billion [111]. In Bypass fraud, fraudsters illegally install or place a SIM Box at its premises. The sim box routes the calls from the international caller to the callee, presenting that call is originated from the local mobile or telephone fixed exchanges, thus bypassing charges paid to the regulator on the international long distance call. This call fraud largely affects the regulator and the end-users in the sense that regulator loses money because of local termination and end-users are paying for the premium call route but the route provided to them is a low-quality route.

In practice, Bypass fraud works in two ways [112, 113]. 1) The fraudster presents himself as the legitimate telecommunication entity to other telecommunication companies. Once the agreement is signed for the interconnect, the terminating operator routes calls from the originating operator via the simbox, which is not observable to the caller and the originating operator. However, over the period of time, the caller could notice the low-quality route because of degraded quality and report it to the operator. 2) The owner of the Simbox network to offer the cheap call termination, though this would not directly impact the caller or the callee in terms of financial loss, it would bring a loss to the regulator and legitimate call termination operators for not receiving share on the calls originating from overseas.

5.2.3. International Revenue Sharing Fraud

In International Revenue Sharing Fraud (IRSF), fraudsters illegally hack or convince a callee to make a call to a premium number. This would not only result in financial loss for telecommunication operators but would also bring loss to end-users and small enterprises.

IRSF fraud can be committed in two ways. 1) the fraudster can trick the callee to call back on the premium numbers by using a stolen identity or making a miscall to the callee [114, 110]. 2) The fraudster uses the resources of hacked telecommunication operator or private branch exchange (PBX) of an enterprise in order to originate calls for the premium number obtained from an International Premium Rate Number provider. With IRSF, fraudsters make repeated calls to premium numbers or international calls to destinations with high termination rates. This results in a loss of around $6.1 billion a year to the enterprise and telecommunication operators [111].

5.2.4. Subscription Frauds

In subscription fraud, the fraudster uses the telecommunication services with the intention of not paying the charges to the telecommunication operators. This is probably a common fraud activity and can be often managed without a huge investment. The fraudsters in a subscription fraud can be grouped into two types: 1) the personal use, i.e buying the subscription services or buy the post-paid sim cards on the stolen identities and have no intentions to pay the bills, 2) for the profit, i.e. selling the long distance calls using acquired sim cards. The subscription fraud is the major problems for telecommunication service providers and accounts for $2 billion which is roughly 40% of all fraud losses [111].

5.2.5. Robo and Telemarketing Calls

A robocall or the telemarketing call is the phone call that uses telecommunication medium and the computerized autodialer to deliver a pre-recorded telemarketing message to the call receiver. These calls are often made for political campaigns, collecting donations, offering holiday packages, promoting political and religious thoughts and selling legal and illegal products. These calls can come at any hour of the day and require an immediate response from the recipient, thus annoy call recipients while at work, disturb them in their family times, and can even interrupt their sleep in late hours at night. Recent statistics on telephony spam have revealed that answering a spam call would result in an estimated loss of 20 million man-hours for a small business enterprise in the United States with the estimated loss of about $475 million annually [115, 116]. In 2016, estimated US residents have received around 2.4 billion robocalls per month [117]. Every year service providers, regulators, and law enforcement agencies receive thousands of complaints from consumers for unsolicited, unauthorized, and fraudulent callers trying to abuse them. These calls can also be the first step towards the frauds. FTC (Federal Trade Communication) has estimated that every year scammers and spammers cause a loss of $8.6 billion annually to citizens of USA due to frauds and majority of them are initiated from the telephone [118]. In 2016, it was estimated that around 27 million U.S. consumers lost approximately $7.4 billion to phone scams and robocalling, averaging $274 per victim [119].

5.2.6. Over the Top Bypass

Over the top (OTT) communication applications are those that operate over the Internet. They provide services like instant messaging, telephony over Internet and streaming video. The OTT apps are widely used by the people for staying connected with friends and making long distance cheap or free telephone calls. WhatsApp, the most popular OTT app for instant messaging and voice communication, has more than 1.5 billion monthly active users [120]. The OTT bypass is similar to the simbox fraud but this fraud is generally done by the telecommunication operators with their customers and termination operators [121]. In this fraud, the telecommunication operator makes an agreement with the OTT provider and divert calls for the receiver through the OTT app instead of diverting them to legitimate telecommunication operators. The operator commits frauds with their customer by charging a premium rate and commit fraud with the termination operators by not paying the legitimate share.

5.3. Systems for Detecting Frauds and Spamming in Telecommunications

In this section we present a discussion on the detection system from two perspectives: 1) systems designed for detecting frauds and 2) systems designed for detecting spam or robocalling.

5.3.1. Fraud Detection Systems

Frauds in telecommunication networks can be identified in two ways: 1) analyzing the call detailed records of the subscribers, 2) analyzing the quality of service features of speech and signaling messages between the caller and the callee. In this section, we discuss some prevalent systems used for identifying frauds in the mobile cellular and telecommunication networks.

The quality of voice call degrades during its conversion from the IP to mobile call. The features of voice quality, delay and signaling delay between the caller and callee is used to identify the simbox or over the top frauds in the mobile cellular networks [122, 121]. It is easy to spoof the caller identity using VoIP systems and modern smartphone applications. The identities of the user can be authenticated using the cryptographic handshake between the caller and the callee [123, 124, 125, 126], using the public key infrastructure [125] and replaying the call to the caller during the call setup phase [127]. However, having a public key infrastructure in a voice network is problematic because of small bandwidth voice channel. The characteristics of speech content [128] can also be used to identify the spoofers and fraudsters but it requires extensive system resources and speech database of legitimate and non-legitimate users.

The collected call detailed records and machine learning approaches could be used together to identify different calling patterns of residential and commercial subscribers [129, 130, 131, 132]. The accuracy and detection performance of these systems mainly depends on the underlying machine learning algorithms and the features used for characterizing the behavior. These systems could identify the fraudsters making calls at a very high rate but could not identify stealthy callers and callers who frequently change their networks. The collaboration among multiple service providers could identify the fraudsters in a timely manner. The collaboration between service providers can be carried out through the exchange of their dataset in a multi-party secure set intersection way [133].

5.3.2. Robo or Telemarketing Call Detection Systems

The service provider deploys a standalone system that analyzes the behavior of the caller within the network. This section outlines some of the standalone systems that have been designed for blocking robo and telemarketers in the service provider network [134, 135, 136]. Readers are encouraged to see [135, 136] for more details on how spam detection systems work and their limitations. In this section, we briefly discuss the working of some prominent detection systems.

In telecommunication networks, the successful call consists of two parts: a signaling part – responsible for establishing the link between the caller and the callee, and the speech exchange part – responsible for exchanging bidirectional speech content between the caller and the callee. In a telecommunication network, the content-based detection system can be applied in two ways: processing speech content in real-time or process speech content after the call. A number of content-based systems have been proposed for detecting spammers in the telecommunication networks [137] [138], [139]. These systems mainly measure the similarity between speech samples in real and non-real time. However, the content-based systems have some limitations: 1) content is only available after the call, but this is late to flag to block the caller as it has already disturbed the callee, 2) requires extensive system resources, 3) it is prohibited by law to monitor and process users speech content.

A C/R (Challenge/Response) system is a system that enables telephony users to solve the given challenge. Humans (legitimate and non-legitimate) can easily solve the challenge initiated by the call handling system, whereas machines would find it far more difficult to solve the challenge. The C/R-based system operates in two modes:1) by having authentication in a non-intrusive way without involving the subscriber [140] and 2) an intrusive way using a CAPTCHA challenge to verify the subscriber [141], [142, 143]. C/R-based approaches are well suited for blocking machine or auto-dialer spammers but its placement in a real-network has problems. Further, it will introduce notable call setup delay which might displease subscriber for each call made.

The list-based systems are identity-based systems that place the subscriber in the white, black or grey list depending on the behavior of the subscriber [144], [145, 146]. The call processing unit checks the nature of the subscriber during the call setup phase. A list database can be either global – applied to all subscribers or personalized – applied to particular subscribers. The list-based approaches need to be implemented along with other approaches that actually make a decision which list the subscriber should be placed in [147], [148], [149]. The limitation of the list-based system is that it needs a continuous update of database and coordination with an underlying detection system for the list database.

The spam caller can also be made barred from calling by imposing a huge financial penalty for their nuisance call. A major limitation of the cost-based system is that it requires a comprehensive micro-payment system for the computation of deduction and holding of money.

Another way to stop unwanted telemarketing calls is to have a Multi-Stage system that establishes an internal collaboration between different standalone approaches [150, 148, 151]. This would improve the detection accuracy and detection time because it uses collective information about caller's behavior from multiple approaches but it could have high call setup delay. Furthermore, the CAPTCHA based multistage systems require interaction with the caller and the callee, thus are intrusive.

The statistics-based detection systems monitor different call statistics of the subscriber during and after the call. These approaches first collect statistics from the raw call detailed records or signaling messages and then apply data mining to characterize the behavior of the caller [152, 153, 154].

Scammers normally use some specialized software and hardware devices which are quite different from devices used by legitimate users. The device fingerprinting could be used to block the spammers by having the database of fingerprints of legitimate and non-legitimate devices at the call processing system [155]. The use of device fingerprinting in real deployment is not practical and scalable as it requires management of fingerprints of a large number of commercial and non-commercial VoIP devices. Additionally, a spammer can bypass fingerprinting-based systems by adopting fingerprints and protocol stack similar to the devices used by the legitimate subscribers.

Scammers use a telephone directory to randomly select their victims. Furthermore, call records to contain sensitive information and it is not legal to use them without user consent. Telephony Honeynet (a network of a virtual number not assigned to any human) could be used to collect the data to be used for characterizing the behavior of the caller in the network, [156], [157]. The honeynet-based solution can identify spammers but these would not be able to identify those spammers spamming other users in the network. The spammers can also bypass honeypot systems by learning the numbering pattern of honey phones or by using phone numbers of real users.

The reputation of legitimate callers increases over time and the reputation of scammers decreases over time because they do not develop a strong social circle with their callees. The reputation of the caller can be computed in two ways: 1) having direct collaboration between subscribers, and 2) deploying a centralized system for handling and processing subscriber feedback. The trust between subscribers can be computed in two ways: 1) intrusive way – that implicitly requires interaction with the call recipients of the subscriber [147],[148],[158, 159] for the feedback about subscriber, and 2) a non-intrusive way – that explicitly utilizes information from call logs recorded for the billing purposes [160]. Reputation-based anti-SPIT systems have shown great effectiveness against spammers in email and VoIP networks but their effectiveness depends on the set of features used for the computation of global reputation. In some cases, a spammer could have reputation scores by creating a Sybil network between their acquired identities and also spoofed identities of the legitimate subscribers.

The simple way to limit spammers to use the network is to define some strong legislation and to impose heavy penalty on the users involved in mass telemarketing and spamming. These legislations prohibit unsolicited communication to reach the recipient unless prior consent from the recipient is obtained. The major limitation of the legislation-based system is the difficulty of tracing back the initiators of spam. Moreover, if the regulator or law enforcement agencies trace-back the initiator of unsolicited communication even then there is no such global law existing that will apply to spammers across the world. Moreover, spammers make spams from anywhere around the world thus making the anti-spam law of one country inapplicable to the spammer spamming from places where no such law exists.

The calling behavior of the subscriber becomes more meaningful when subscribers are observed across many service providers. Naturally, collaboration among service providers would improve the detection time and detection accuracy because of the collective use of information from many autonomous collaborating service providers. A few works have been reported that incorporate collaboration among service providers for rating the subscribers [161] [162][163] [164, 165]. These systems could improve detection accuracy but bring the challenges of privacy preservation and collaboration overheads.

6. Way forward To Minimize Frauds

Cybercriminals and scammers continuously change their attack strategies and use loopholes in the technology to have a high success rate. In this section, we highlight some challenges that need to be addressed to minimize cyber frauds.

6.1. Identity spoofing In Telecommunications

Cybercriminals normally have a large number of identities as well as have the ability to spoof the identity of the legitimate entities, for example, banks, social security, and tax departments. Although the identity of the users over the social networks, web, and email may be verified by using the public key infrastructure and transport layer protocols, people are unaware of its working, presentation of credentials and the verification process. The unawareness of the protocol behavior would still lead to an increase of victims of spear phishing and social engineering attacks. Furthermore, as stated, nowadays the telephony networks (mobile, landline and VoIP) have become the most preferred way to stay in contact with family, friends, and colleagues and doing business in the real time. The criminals are also utilizing this medium to defraud users out of money. Furthermore, the telephony network has also been used for the exchange of private information e.g. two-factor authentication, exchange of one-time bank transaction codes or passcode and communicating for some sensitive task. The telephony system is secure to some extent, but it does not provide any mechanism for identity verification that enables users to verify who is on the other side of the call. The challenges in the design of verification and authentication for telephony are two-fold: 1) to achieve authentication without using the public key infrastructure, 2) to enable users to authenticate without any additional call setup delay. The challenge in the former is who should act as the "trusted" certifying authority in the PKI. This can be achieved by employing the self-enforcing mechanism that authenticates the end-user through the exchange of small bit code between end-users for example DTMF tone. The user can also be authenticated by using the behavioral features extracted from the speech samples of the users, but this is the second stage detection and there are chances that users have already been affected by the spoofed identity.

6.2. Spear Phishing

Cybercriminals are intelligent and use new techniques to bypass the trust of their victims. One such techniques cybercriminals are using is the spear phishing where they pretend that they are also part of the organization, company or social network group of the victim. Through spear phishing, the attacker can convince victims to disclose their private information, which then is then used for financial fraud. In the case of spear phishing, however, the source of the email is likely to be known to the target that makes him trust the information in the email. To overcome this attack, there is a need to train the users about verifying the email headers of the source. This becomes more challenging for the people who do not know about the working of the technology. The users should also be informed about the risk of sharing the information over the social media sites which can be used for a sophisticated spear phishing attack.

6.3. Collaboration

Collaboration among service providers and users could considerably improve the defense against the cybercriminals. However, there is no such mechanism existing that enables financial institutions, government organizations and end-users to effectively collaborate with each other for the collaborative defense against cybercriminals. Furthermore, organizations are also reluctant to collaborate because of privacy concerns and they are competitors to each other. The challenge in the design of a collaborative system is that it should provide a setup that ensures the privacy and integrity of data provided by the collaborators. One possible way to achieve privacy-preserving collaboration is to have a cryptographic system along with the use of blockchain. This collaboration would ensure privacy and security of collaborator which convince them to the part in the collaboration process. The can be achieved by having the regulator that ensures that participants are participating in an honest way and not maliciously using the collaboration as the tool to attack each other.

6.4. Cyber Education and Training

The cybercriminals often use social engineering attacks and emotional sentiments to defraud their targets. Elderly people are more vulnerable to be attacked and are victims of such an attack. It is important that financial entities and organizations should have a mechanism to provide training (in the form of video or poster) to their customers time, for example at the time when a customer registers with them. Further, it is also recommended that financial institutions should have two-factor authentication for the transfer of money from old age customers.

7. Conclusions

Globally, consumers over Internet technologies lose millions to cybercrime per year. Similarly, the service providers and regulators have also spent billions of dollars for the defense mechanism to safeguard the consumers from frauds and malicious activities. At present, there is little information available about how the fraudsters work, and how fraud happens over Internet technologies. This paper is the first attempt to analyze the attack mechanism of fraudsters and the defenses deployed by the service providers to protect their users from the fraud. We chose three technologies i.e. Payment card fraud, mobile payment frauds, and telephone frauds because of high penetration and their usage in the daily life activities and their inter-connection (personal information is often leaked via the telephone fraud and is subsequently used in payment fraud). To this extent, we provided a comprehensive discussion on mechanisms used by fraudsters to defraud the users over these technologies, the economic impact of frauds over and the public and the service providers and the defense mechanism. Today consumers are more vulnerable to fraud and cybercrimes because of the usage of a diverse set of technologies in our daily life e.g. mobile applications, Internet of Things, and virtual assistance device. The consumer becomes the victim because of many attack vectors such as social engineering attacks and vulnerabilities in mobile devices. We believe that securing these systems is the shared responsibility between the consumers, regulators and service providers. The service providers should have an updated defense mechanism, should provide a frequent update to their consumers through education. The responsibility of the regulator is to provide a collaborative platform where service providers can share the latest attack mechanism and vulnerabilities in the systems for efficient attack detection. The consumers should also be provided with training about not providing private personal details to an unknown person over the Internet. We believe adopting collaborative security and consumer training would help protect the consumers from the cybercrime effectively.

section*Acknowledgment Muhammad Ajmal Azad and Feng Hao are supported by the ERC Starting Grant, No. 306994. We thank the anonymous reviewers for their insightful comments and suggestions.

References

[1] (2016, 01, December) 2017 internet crime report. [Online]. Available: https://goo.gl/MUNzTM

[2] McAfee, "Economic Impact of CybercrimeNo Slowing Down Report," 2018. [Online]. Available: https://goo.gl/QLjj8H

[3] (2018, 01, December) 2017 norton cyber security insights report global results. [Online]. Available: https://goo.gl/nF88NN

[4] M. Kaakinen, T. Keipi, P. Rsnen, and A. Oksanen, "Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults," *Cyberpsychology, Behavior, and Social Networking*, vol. 21, 10 2017.

[5] (2016) The cost of cyber crime. [Online]. Available: https://goo.gl/gFe4gw

[6] (2018, 01, December) How to spot tech support scams. [Online]. Available: https://goo.gl/FLrEeQ

[7] (2018, 01, December) Microsoft cites 24% jump in tech support scams. [Online]. Available: https://goo.gl/kzKFiE

[8] I. Yaqoob, E. Ahmed, M. H. ur Rehman, A. I. A. Ahmed, M. A. Al-garadi, M. Imran, and M. Guizani, "The rise of ransomware and emerging security challenges in the internet of things," *Computer Networks*, vol. 129, pp. 444 – 458, 2017, special Issue on 5G Wireless Networks for IoT and Body Sensors.

[9] M. Xu, K. M. Schweitzer, R. M. Bateman, and S. Xu, "Modeling and predicting cyber hacking breaches," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2856–2871, 2018.

[10] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. A. Kazmi, and C. S. Hong, "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Generation Computer Systems*, vol. 92, pp. 265 – 275, 2019.

[11] K. Modi and R. Dayma, "Review on fraud detection methods in credit card transactions," in *2017 International Conference on Intelligent Computing and Control (I2C2)*, June 2017, pp. 1–5.

[12] (2016, 01, December) 2017 the nelson report. [Online]. Available: https://goo.gl/HSmyha

[13] (2016, 01, December) Communications Fraud Control association (CFCA) Announces Results of Worldwide Telecom Fraud Survey published in 2016. [Online]. Available: https://goo.gl/H1VLae
[14] "National initiative for cybersecurity careers and studies explore terms in cybersecurity terminology," 2017. [Online]. Available: https://goo.gl/Ehnt5i
[15] "Nistir glossary of key information security terms," 2017. [Online]. Available: https://goo.gl/DWxg35
[16] T. J. Holt, G. W. Burruss, and A. M. Bossler, "Assessing the macro-level correlates of malware infections using a routine activities framework," *International Journal of Offender Therapy and Comparative Criminology*, vol. 62(6), p. 17201741, 2018.
[17] M. A. Azad, S. Bag, and F. Hao, "Privbox: Verifiable decentralized reputation system for online marketplaces," *Future Generation Computer Systems*, vol. 89, pp. 44 – 57, 2018.
[18] "E-commerce fraud rates spike 33% in 2016," 2017. [Online]. Available: https://goo.gl/YjFgnk
[19] "Fraud facts 2017recognize, reject, report fraud," 2017. [Online]. Available: http://www.competitionbureau.gc.ca
[20] "Online bargain hunters buy even if they think it may be a scam," 2017. [Online]. Available: https://goo.gl/81PLgw
[21] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the mirai botnet," in *Proceedings of the 26th USENIX Conference on Security Symposium*, ser. SEC'17. Berkeley, CA, USA: USENIX Association, 2017, pp. 1093–1110.
[22] A. Fadele, M. Othman, I. Hashem, I. Yaqoob, M. Imran, and M. Shoaib, "A novel countermeasure technique for reactive jamming attack in internet of things," *Multimedia Tools and Applications*, 09 2018.
[23] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.
[24] L. O. Mailloux and M. Grimaila, "Advancing cybersecurity: The growing need for a cyber-resiliency workforce," *IT Professional*, vol. 20, no. 3, pp. 23–30, May 2018.
[25] "The Nilson Report on Card Fraud," 2017. [Online]. Available: https://goo.gl/8m61Wc
[26] "Statista - U.S. payment card fraud losses by type 2018." [Online]. Available: https://goo.gl/p1ksPe
[27] FICO, "EVOLUTION OF CARD FRAUD IN EUROPE 2016," 2018. [Online]. Available: http://www.fico.com/europeanfraud/
[28] Council of the European Union, "EU Policy Cycle for Organised and Serious International Crime 2018/2021," 2017. [Online]. Available: https://goo.gl/xuVqpU
[29] Financialfraudactionuk, "THE DEFINITIVE OVERVIEW OF PAYMENT INDUSTRY FRAUD," 2016. [Online]. Available: https://goo.gl/qtHm6P
[30] EMV, "Home - EMVCo." [Online]. Available: https://www.emvco.com/
[31] IBM, "VISA PIN Algorithms." [Online]. Available: https://goo.gl/4AJ1mf
[32] K. Mayes and K. Markantonakis, Eds., *Smart Cards, Tokens, Security and Applications.* Cham: Springer International Publishing, 2017.
[33] Martin Emms, "Contactless payments :usability at the cost of security?" Ph.D. dissertation, Newcastle Univeristy. [Online]. Available: https://theses.ncl.ac.uk/dspace/handle/10443/3304
[34] EMVCo, "EMV Integrated Circuit Card Specifications for Payment Systems," *Book 1*, vol. 4.3, 2011.
[35] "ATM Shimmers' Target Chip-Based Cards Krebs on Security." [Online]. Available: https://goo.gl/FoNrYq
[36] S. J. Murdoch, S. Drimer, R. Anderson, and M. Bond, "Chip and PIN is Broken," in *2010 IEEE Symposium on Security and Privacy.* IEEE, 2010, pp. 433–446.
[37] LeParisien, "L'imparable escroquerie à la carte bancaire - Le Parisien," 2012. [Online]. Available: https://goo.gl/cBNb8t
[38] EMVCo, "EMV Contactless Interface Specification," *Book C1-C7*, vol. 3.0, 2019.
[39] Martin Emms, "Contactless payments :usability at the cost of security?" Ph.D. dissertation, Newcastle Univeristy. [Online]. Available: https://theses.ncl.ac.uk/dspace/handle/10443/3304

[40] M. Emms, B. Arief, L. Freitas, J. Hannon, and A. van Moorsel, "Harvesting High Value Foreign Currency Transactions from EMV Contactless Credit Cards Without the PIN," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14*. New York, New York, USA: ACM Press, 2014, pp. 716–726. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2660267.2660312

[41] L. Delamaire, H. Abdou, and J. Pointon, "Credit card fraud and detection techniques: a review," *Banks and Bank Systems*, vol. 4, no. 2, pp. 57–68, April 2009. [Online]. Available: http://eprints.hud.ac.uk/id/eprint/19069/

[42] R. Broadhurst, P. Grabosky, M. Alazab, B. Bouhours, and S. Chon, "Organizations and cybercrime: An analysis of the nature of groups engaged in cybercrime," *International Journal of Cyber Criminology*, vol. 8, pp. 1–20, 03 2014.

[43] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 2006, pp. 581–590.

[44] S. Egelman, L. F. Cranor, and J. Hong, "You've been warned: an empirical study of the effectiveness of web browser phishing warnings," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2008, pp. 1065–1074.

[45] S. Tajalizadehkhoob, H. Asghari, C. Gañán, and M. Van Eeten, "Why them? extracting intelligence about target selection from zeus financial malware," in *Proceedings of the 13th Annual Workshop on the Economics of Information Security, WEIS 2014, State College (USA), June 23-24, 2014*. WEIS, 2014.

[46] N. Etaher, G. R. Weir, and M. Alazab, "From zeus to zitmo: Trends in banking malware," in *Trustcom/BigDataSE/ISPA, 2015 IEEE*, vol. 1. IEEE, 2015, pp. 1386–1391.

[47] W. Gharibi and A. Mirza, "Software vulnerabilities, banking threats, botnets and malware self-protection technologies," *arXiv preprint arXiv:1105.1720*, 2011.

[48] M. Yip, C. Webber, and N. Shadbolt, "Trust among cybercriminals? carding forums, uncertainty and implications for policing," *Policing and Society*, vol. 23, no. 4, pp. 516–539, 2013.

[49] M. Yip, N. Shadbolt, and C. Webber, "Structural analysis of online criminal social networks," 2012.

[50] ISO, "ISO/IEC 7816-4:2013 - Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange." [Online]. Available: https://www.iso.org/standard/54550.html

[51] "ISO/IEC 14443-3:2011 - Identification cards – Contactless integrated circuit cards – Proximity cards – Part 3: Initialization and anticollision." [Online]. Available: https://www.iso.org/standard/50942.html

[52] M. A. Ali, B. Arief, M. Emms, and A. van Moorsel, "Does the Online Card Payment Landscape Unwittingly Facilitate Fraud?" *IEEE Security & Privacy*, vol. 15, no. 2, pp. 78–86, mar 2017.

[53] "ISO/IEC 7812-1:2017 - Identification cards – Identification of issuers – Part 1: Numbering system." [Online]. Available: https://www.iso.org/standard/70484.html

[54] "ISO 10202-6:1994 - Financial transaction cards – Security architecture of financial transaction systems using integrated circuit cards – Part 6: Cardholder verification." [Online]. Available: https://www.iso.org/standard/18233.html

[55] "ISO 10202-6:1994 - Financial transaction cards – Security architecture of financial transaction systems using integrated circuit cards – Part 6: Cardholder verification." [Online]. Available: https://www.iso.org/standard/18233.html

[56] "ISO 10202-6:1994 - Financial transaction cards – Security architecture of financial transaction systems using integrated circuit cards – Part 6: Cardholder verification." [Online]. Available: https://www.iso.org/standard/18233.html

[57] PYMNTS, "MOBILE COMMERCEAs Mobile Commerce Grows, M-Commerce Fraud Grows Even Faster," 2015. [Online]. Available: https://goo.gl/3gmYE7

[58] T. Dahlberg, N. Mallat, J. Ondrus, and A. Zmijewska, "Past, present and future of mobile payments research: A literature review," *Electronic Commerce Research and Applications*, vol. 7, no. 2, pp. 165 – 181, 2008, special Section: Research Advances for the Mobile Payments Arena.

[59] (2016, 01, December) More than one in 10 employees fall for social engineering attacks. [Online].

Available: https://goo.gl/EpCswV

[60] (2016, 01, December) Be warned: Scammers are making fake versions of your favorite apps to steal your data. [Online]. Available: https://goo.gl/6aq9T9

[61] M. Alazab, S. Venkatraman, P. Watters, M. Alazab, and A. Alazab, "Cybercrime: The case of obfuscated malware," in *Global Security, Safety and Sustainability & e-Democracy*, C. K. Georgiadis, H. Jahankhani, E. Pimenidis, R. Bashroush, and A. Al-Nemrat, Eds. Springer Berlin Heidelberg, 2012.

[62] R. business-driven security, "RSA Quaterly fraud report Q1 2018," Tech. Rep. 1, 2018. [Online]. Available: https://goo.gl/cRucvx

[63] LexisNexis, "True Cost of Fraud Study," Tech. Rep. May, 2016. [Online]. Available: https://goo.gl/Hrfx17

[64] K. T. F. P. Braintree, "MOBILE PAYMENTS 2018 Report," Tech. Rep., 2018. [Online]. Available: https://goo.gl/MJbMFU

[65] Statista.com, "Number of apps available in leading app stores as of 1st quarter 2018," 2018. [Online]. Available: https://goo.gl/8FHr3t

[66] F. Hannah, "Massive spike in mobile app fraud," *lovelymoney.com*, 2018. [Online]. Available: https://goo.gl/ksiybg

[67] K. Fitzgerald, "Data: The new causes of mobile payments fraud," 2018. [Online]. Available: https://goo.gl/snazqJ

[68] S. Ragan, "Equifax says website vulnerability exposed 143 million US consumers," *csonline.com*, 2017.

[69] M. Haber, "Password Reuse Overcome the Vulnerability," *Beyondtrust.com*, 2016. [Online]. Available: https://goo.gl/FGeqPG

[70] J. Pagliery, "Hackers are draining bank accounts via the Starbucks app," may 2015. [Online]. Available: https://goo.gl/G7EDgu

[71] C. F. Jr, "Phishing Threats Move to Mobile Devices," *darkreading.com*, 2018. [Online]. Available: https://goo.gl/2vn3rH

[72] (2016, 01, December) Mobile users 3 times more vulnerable to phishing attacks. [Online]. Available: https://goo.gl/gHxDtm

[73] (2016, 01, December) Majority of emails opened on apple devices, android users pay more attention. [Online]. Available: https://goo.gl/J3fCco

[74] M. Mehrnezhad, M. A. Ali, F. Hao, and A. van Moorsel, "Nfc payment spy: A privacy attack on contactless payments," in *Security Standardisation Research*, L. Chen, D. McGrew, and C. Mitchell, Eds. Cham: Springer International Publishing, 2016, pp. 92–111.

[75] M. Boodaei, "Mobile Users 3 Times More Vulnerable to Phishing Attacks," 2011. [Online]. Available: https://goo.gl/ksQCKA

[76] A. Felt and D. Wagner, "Phishing on mobile devices," *presentation at W2SP: Web*, vol. 2, pp. 1–10, 2011.

[77] M. Koschuch, M. Hudler, H. Eigner, and Z. Saffer, "Token-based authentication for smartphones," in *2013 International Conference on Data Communication Networking (DCNET)*, July 2013, pp. 1–6.

[78] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M.-E. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich, "Back-of-device authentication on smartphones," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '13. New York, NY, USA: ACM, 2013, pp. 2389–2398.

[79] T. Feng, Z. Liu, K. A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen, "Continuous mobile authentication using touchscreen gestures," in *2012 IEEE Conference on Technologies for Homeland Security (HST)*, Nov 2012, pp. 451–456.

[80] P. Dunphy, A. P. Heiner, and N. Asokan, "A closer look at recognition-based graphical passwords on mobile devices," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ser. SOUPS '10. New York, NY, USA: ACM, 2010, pp. 3:1–3:12.

[81] Q. Akariman, A. N. Jati, and A. Novianty, "Face recognition based on the android device using lbp algorithm," in *2015 International Conference on Control, Electronics, Renewable Energy and*

Communications (ICCEREC), Aug 2015, pp. 166–170.

[82] Y. Shen, W. Hu, M. Yang, B. Wei, S. Lucey, and C. T. Chou, "Face recognition on smartphones via optimised sparse representation classification," in *IPSN-14 Proceedings of the 13th International Symposium on Information Processing in Sensor Networks*, April 2014, pp. 237–248.

[83] K. Patel, H. Han, and A. K. Jain, "Secure face unlock: Spoof detection on smartphones," vol. 11, 06 2016.

[84] M. Trokielewicz, "Iris recognition with a database of iris images obtained in visible light using smartphone camera," in *2016 IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*, Feb 2016, pp. 1–6.

[85] K. B. Raja, R. Raghavendra, and C. Busch, "Smartphone based robust iris recognition in visible spectrum using clustered k-means features," in *2014 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS) Proceedings*, Oct 2014, pp. 15–21.

[86] R. Raghavendra and C. Busch, "Learning deeply coupled autoencoders for smartphone based robust periocular verification," in *2016 IEEE International Conference on Image Processing (ICIP)*, Sept 2016, pp. 325–329.

[87] M. Chaa, N. E. Boukezzoula, A. Meraoumia, and M. Korichi, "An efficient biometric based personal authentication system using finger knuckle prints features," in *2016 International Conference on Information Technology for Organizations Development (IT4OD)*, March 2016, pp. 1–5.

[88] N. Zirjawi, Z. Kurtanovic, and W. Maalej, "A survey about user requirements for biometric authentication on smartphones," in *2015 IEEE 2nd Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE)*, Aug 2015, pp. 1–6.

[89] N. Shabrina, T. Isshiki, and H. Kunieda, "Fingerprint authentication on touch sensor using phase-only correlation method," in *2016 7th International Conference of Information and Communication Technology for Embedded Systems (IC-ICTES)*, March 2016, pp. 85–89.

[90] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, and S. Ben-David, "Biometric authentication on a mobile device: A study of user effort, error and task disruption," in *Proceedings of the 28th Annual Computer Security Applications Conference*, ser. ACSAC '12. New York, NY, USA: ACM, 2012, pp. 159–168.

[91] C. Nickel, H. Brandt, and C. Busch, "Benchmarking the performance of svms and hmms for accelerometer-based biometric gait recognition," in *2011 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, Dec 2011, pp. 281–286.

[92] M. Parreño-Centeno, Y. Guan, and A. van Moorsel, "Mobile Based Continuous Authentication Using Deep Features," *Procedings of 2nd Int. Work. Embed. Mob. Deep Learn.*, p. 6, 2018.

[93] N. Neverova, C. Wolf, G. Lacey, L. Fridman, D. Chandra, B. Barbello, and G. Taylor, "Learning Human Identity from Motion Patterns," *IEEE Access*, vol. 4, pp. 1810–1820, 2016.

[94] K. B. Raja, R. Raghavendra, M. Stokkenes, and C. Busch, "Multi-modal authentication system for smartphones using face, iris and periocular," in *2015 International Conference on Biometrics (ICB)*, May 2015, pp. 143–150.

[95] M. Parreño-Cenetno, S. Castruccio, and A. van Moorsel, "Smartphone Continuous Authentication Using Deep Learning Autoencoders," *Privacy, Security and Trust 2017*, 2017.

[96] H. Xu, Y. Zhou, and M. R. Lyu, "Towards continuous and passive authentication via touch biometrics: An experimental study on smartphones," in *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, ser. SOUPS'14. Berkeley, CA, USA: USENIX Association, 2014, pp. 187–198.

[97] L. Yiyan, Z. Fang, S. Wenhua, and L. Haiyong, "An hidden markov model based complex walking pattern recognition algorithm," in *2016 Fourth International Conference on Ubiquitous Positioning, Indoor Navigation and Location Based Services (UPINLBS)*, Nov 2016, pp. 223–229.

[98] C. Nickel, T. Wirtl, and C. Busch, "Authentication of smartphone users based on the way they walk using k-nn algorithm," in *2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, July 2012, pp. 16–20.

[99] A. Roy, T. Halevi, and N. Memon, "An hmm-based multi-sensor approach for continuous mobile authentication," in *MILCOM 2015 - 2015 IEEE Military Communications Conference*, Oct 2015, pp.

1311–1316.
[100] D. Cilia and F. Inguanez, "Multi-model authentication using keystroke dynamics for smartphones," in *2018 IEEE 8th International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*, Sep. 2018, pp. 1–6.
[101] L. Lu and Y. Liu, "Safeguard: User reauthentication on smartphones via behavioral biometrics," *IEEE Transactions on Computational Social Systems*, vol. 2, no. 3, pp. 53–64, Sep. 2015.
[102] T. Datta and K. Manousakis, "Using svm for user profiling for autonomous smartphone authentication," in *2015 IEEE MIT Undergraduate Research Technology Conference (URTC)*, Nov 2015, pp. 1–5.
[103] J. Sun, K. Yan, X. Liu, C. Yang, and Y. Fu, "Malware detection on android smartphones using keywords vector and svm," in *2017 IEEE/ACIS 16th International Conference on Computer and Information Science (ICIS)*, May 2017, pp. 833–838.
[104] Y. Lu, C. Kuo, H. Chen, C. Chen, and S. Chou, "A svm-based malware detection mechanism for android devices," in *2018 International Conference on System Science and Engineering (ICSSE)*, June 2018, pp. 1–6.
[105] K. Xin, G. Li, Z. Qin, and Q. Zhang, "Malware detection in smartphone using hidden markov model," in *2012 Fourth International Conference on Multimedia Information Networking and Security*, Nov 2012, pp. 857–860.
[106] C. Bo, L. Zhang, T. Jung, J. Han, X.-Y. Li, and Y. Wang, "Continuous User Identification via Touch and Movement Behavioral Biometrics," *Performance Computing and Commun.Conf. (IPCCC), IEEE Int..*, no. 61428203, pp. 1–8, 2014.
[107] Z. Sitova, J. Sedenka, Q. Yang, G. Peng, G. Zhou, P. Gasti, and K. S. Balagani, "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 877–892, may 2016. [Online]. Available: http://ieeexplore.ieee.org/document/7349202/
[108] (2016, 01, December) Number of mobile subscribers worldwide hits 5 billion. [Online]. Available: https://goo.gl/o3JNu4
[109] (2016, 01, December) Number of fixed telephone lines worldwide from 2000 to 2017 (in millions). [Online]. Available: https://goo.gl/rbUbWb
[110] (2016, 01, December) Mobile phone scam kills curious cats. [Online]. Available: https://goo.gl/i2KSTH
[111] (2018, 01, December) 2017 estimated fraud losses by type (in usd billions). [Online]. Available: https://goo.gl/yh2uhu
[112] B. Reaves, E. Shernan, A. Bates, H. Carter, and P. Traynor, "Boxed out: Blocking cellular interconnect bypass fraud at the network edge," in *Proceedings of the 24th USENIX Conference on Security Symposium*, ser. SEC'15. Berkeley, CA, USA: USENIX Association, 2015, pp. 833–848.
[113] M. Sahin, A. Francillon, P. Gupta, and M. Ahamad, "Sok: Fraud in telephony networks," in *2017 IEEE European Symposium on Security and Privacy (EuroS P)*, April 2017, pp. 235–250.
[114] (2018, 01, December) Unexpected missed calls from overseas numbers. [Online]. Available: https://goo.gl/YtKNuz
[115] Spam Phone Calls Cost U.S. Small Businesses Half-Billion Dollars in Lost Productivity, Marchex Study Finds. [Online]. Available: http://goo.gl/jTrgp3
[116] M. Alazab and R. Broadhurst, *The Role of Spam in Cybercrime: Data from the Australian Cybercrime Pilot Observatory*. London: Palgrave Macmillan UK, 2015, pp. 103–120.
[117] The Fight to Eliminate Unwanted Robocalls. [Online]. Available: https://www.aarp.org/content/dam/aarp/ppi/2017/10/the-fight-to-eliminate-unwanted-robocalls.pdf
[118] P. Gupta, R. Perdisci, and M. Ahamad, "Towards measuring the role of phone numbers in twitter-advertised spam," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ser. ASIACCS '18. New York, NY, USA: ACM, 2018, pp. 285–296.
[119] (2018, 01, December) Top consumer phone scams. [Online]. Available: https://goo.gl/r26X5P

[120] Number of monthly active WhatsApp users worldwide from April 2013 to December 2017 (in millions). [Online]. Available: https://goo.gl/ZA5sdF

[121] M. Sahin and A. Francillon, "Over-the-top bypass: Study of a recent telephony fraud," in *Proceedings of the 2016 ACM t SIGSAC Conference on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: ACM, 2016, pp. 1106–1117.

[122] B. Reaves, E. Shernan, A. Bates, H. Carter, and P. Traynor, "Boxed out: Blocking cellular interconnect bypass fraud at the network edge," in *Proceedings of the 24th USENIX Conference on Security Symposium*, ser. SEC'15. Berkeley, CA, USA: USENIX Association, 2015, pp. 833–848.

[123] B. Reaves, L. Blue, and P. Traynor, "Authloop: End-to-end cryptographic authentication for telephony over voice channels," in *25th USENIX Security Symposium (USENIX Security 16).* Austin, TX: USENIX Association, 2016, pp. 963–978.

[124] B. Reaves, L. Blue, H. Abdullah, L. Vargas, P. Traynor, and T. Shrimpton, "Authenticall: Efficient identity and content authentication for phone calls," in *26th USENIX Security Symposium (USENIX Security 17).* Vancouver, BC: USENIX Association, 2017, pp. 575–592.

[125] H. Tu, A. Doupe, Z. Zhao, and G. J. Ahn, "Toward standardization of authenticated caller id transmission," *IEEE Communications Standards Magazine*, vol. 1, no. 3, pp. 30–36, SEPTEMBER 2017.

[126] M. A. Azad and S. Bag, "Decentralized privacy-aware collaborative filtering of smart spammers in a telecommunication network," in *Proceedings of the Symposium on Applied Computing*, ser. SAC '17. New York, NY, USA: ACM, 2017, pp. 1711–1717. [Online]. Available: http://doi.acm.org/10.1145/3019612.3019792

[127] H. Mustafa, W. Xu, A. R. Sadeghi, and S. Schulz, "You can call but you can't hide: Detecting caller id spoofing attacks," in *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, June 2014, pp. 168–179.

[128] V. A. Balasubramaniyan, A. Poonawalla, M. Ahamad, M. T. Hunter, and P. Traynor, "Pindr0p: Using single-ended audio features to determine call provenance," in *Proceedings of the 17th ACM Conference on Computer and Communications Security*, ser. CCS '10. New York, NY, USA: ACM, 2010, pp. 109–120. [Online]. Available: http://doi.acm.org/10.1145/1866307.1866320

[129] H. Farvaresh and M. M. Sepehri, "A data mining framework for detecting subscription fraud in telecommunication," *Engineering Applications of Artificial Intelligence*, vol. 24, no. 1, pp. 182 – 194, 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0952197610001144

[130] S. Y. Sohn and Y. Kim, "Searching customer patterns of mobile service using clustering and quantitative association rule," *Expert Systems with Applications*, vol. 34, no. 2, pp. 1070 – 1077, 2008. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0957417406003939

[131] D. Xing and M. Girolami, "Employing latent dirichlet allocation for fraud detection in telecommunications," *Pattern Recognition Letters*, vol. 28, no. 13, pp. 1727 – 1734, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016786550700147X

[132] M. A. Azad and R. Morla, "Caller-rep: Detecting unwanted calls with caller social strength," *Computers & Security*, vol. 39, pp. 219 – 236, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404813001090

[133] W. Henecka and M. Roughan, "Privacy-preserving fraud detection across multiple phone record databases," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 6, pp. 640–651, Nov 2015.

[134] A. Keromytis, "A Comprehensive Survey of Voice over IP Security Research," *IEEE Communications Surveys Tutorials*, vol. PP, no. 99, pp. 1 –24, 2011.

[135] H. Tu, A. Doupé, Z. Zhao, and G. Ahn, "SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam," in *37th IEEE Symposium on Security and Privacy*, 2016.

[136] M. A. Azad, R. Morla, and K. Salah, "Systems and methods for spit detection in voip: Survey and future directions," *Computers & Security*, vol. 77, pp. 1 – 20, 2018.

[137] S. Iranmanesh, H. Sengar, and H. Wang, "A Voice Spam Filter to Clean Subscribers? Mailbox," in *Security and Privacy in Communication Networks.* Springer, 2013, pp. 349–367.

[138] J. Strobl, B. Mainka, G. Grutzek, and H. Knospe, "An Efficient Search Method for the Content-based

Identification of Telephone-SPAM," in *2012 IEEE ICC*, 2012, pp. 2623–2627.

[139] D. Lentzen, G. Grutzek, H. Knospe, and C. Porschmann, "Content-Based Detection and Prevention of Spam over IP Telephony - System Design, Prototype and First Results," in *2011 IEEE ICC*, 2011, pp. 1–5.

[140] K. Srivastava and H. Schulzrinne, "Preventing Spam for SIP-based Instant Messages and Sessions," Columbia University Technical Report CUCS-042-04, Tech. Rep., October 2004.

[141] J. Lindqvist and M. Komu, "Cure for Spam Over Internet Telephony," in *4th IEEE CCNC*, 2007.

[142] J. Quittek, S. Niccolini, S. Tartarelli, and R. Schlegel, "On Spam over Internet Telephony (SPIT) Prevention," in *IEEE Communications Magazine*, 2008, pp. 80–86.

[143] Y. Soupionis, R. Koutsiamanis, P. Efraimidis, and D. Gritzalis, "A Game-theoretic Analysis of Preventing Spam over Internet Telephony via Audio CAPTCHA-based Authentication," *Journal Computer Security*, vol. 22, pp. 383–413, 2014.

[144] M. Hansen, M. Hansen, J. Möller, T. Rohwer, C. Tolkmit, and H. Waack, "Developing a Legally Compliant Reachability Management System as a Countermeasure against SPIT," in *3rd Annual VoIP Security Workshop*, 2006.

[145] D. Shin, J. Ahn, and C. Shim, "Progressive Multi Gray-Leveling: a Voice Spam Protection Algorithm," in *IEEE Network*, 2006, pp. 18–24.

[146] S. Pandit, R. Perdisci, M. Ahamad, and P. Gupta, "Towards measuring the effectiveness of telephony blacklists"," in *Proceedings of the Network and Distributed System Security Symposium, NDSS 2018*. New York, NY, USA: ACM.

[147] P. Kolan and R. Dantu, "Socio-Technical Defense Against Voice Spamming," *ACM Transactions on Autonomous and Adaptive Systems*, vol. 2, 2007.

[148] R. Dantu and P. Kolan, "Detecting Spam in VoIP Networks," in *The Steps to Reducing Unwanted Traffic on the Internet*, 2005.

[149] K. Ono and H. Schulzrinne, "Have I met you before?: using Cross-Media Relations to Reduce SPIT," in *3rd IPTCOMM*, 2009, pp. 1–7.

[150] R. Schlegel, S. Niccolini, S. Tartarelli, and M. Brunner, "SPam over Internet Telephony (SPIT) Prevention Framework," in *IEEE GLOBECOM*, 2006, pp. 1–6.

[151] M. Azad and R. Morla, "Multistage SPIT Detection in Transit VoIP," in *19th IEEE SoftCOM*, 2011, pp. 1–9.

[152] K. Toyoda and I. Sasase, "SPIT Callers Detection with Unsupervised Random Forests Classifier," in *IEEE ICC*, 2013, pp. 2068–2072.

[153] J. Liu, B. Rahbarinia, R. Perdisci, H. Du, and L. Su, "Augmenting telephone spam blacklists by mining large cdr datasets," in *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ser. ASIACCS '18. New York, NY, USA: ACM, 2018, pp. 273–284.

[154] J. Zhang, J. Wang, Y. Zhang, J. Xu, and H. Wu, "A novel spitters detection approach with unsupervised density-based clustering," in *Data Mining and Big Data*, Y. Tan, Y. Shi, and Q. Tang, Eds. Cham: Springer International Publishing, 2018, pp. 314–324.

[155] H. Hong, K. Sripanidkulchai, H. Zhang, Z. Shae, and D. Saha, "Incorporating Active Fingerprinting into SPIT Prevention Systems," in *VSW06*, 2006.

[156] P. Gupta, B. Srinivasan, V. Balasubramaniyan, and M. Ahamad, "Phoneypot: Data-driven Understanding of Telephony Threats," in *20th NDSS*, 2015.

[157] M. Balduzzi, P. Gupta, L. Gu, Gao.D, and M. Ahamad, "MobiPot: Understanding Mobile Telephony Threats with Honeycards," in *In Proceedings of the 11th ACM ASIACCS*, 2016.

[158] Y. Wu, S. Bagchi, N. Singh, and R. Wita, "Spam Detection in Voice- Over-IP Calls through Semi-Supervised Clustering," in *39th Annual IEEE/IFIP DSN*, 2009, pp. 307–316.

[159] H. Li, X. Xu, C. Liu, T. Ren, K. Wu, X. Cao, W. Zhang, Y. Yu, and D. Song, "A machine learning approach to prevent malicious calls over telephony networks," in *2018 IEEE Symposium on Security and Privacy (SP)*, vol. 00, pp. 561–577.

[160] V. Balasubramaniyan, M. Ahamad, and H. Park, "CallRank: Combating SPIT Using Call Duration, Social Networks and Global Reputation," in *4th CEAS*, 2007.

[161] *Study of Mechanisms for Protection against Unsolicited Communication for IMS (PUCI)*, 3GPP Std.
[162] *Study of Mechanisms for Protection against Unsolicited Communication for IMS (PUCI)*, 3GPP Std. Release 11.
[163] A. Schmidt, A. Leicher, Y. Shah, I. Cha, and L. Guccione, "Sender Scorecards for the Prevention of Unsolicited Communication," in *2nd IEEE Workshop onCollaborative Security Technologies*, 2010, pp. 1–6.
[164] M. Ajmal, S. Bag, S. Tabassum, and F. Hao, "privy: Privacy preserving collaboration across multiple service providers to combat telecoms spam," *IEEE Transactions on Emerging Topics in Computing*, pp. 1–1, 2017.
[165] M. A. Azad and R. Morla, "Rapid detection of spammers through collaborative information sharing across multiple service providers," *Future Generation Computer Systems*, 2018.

Appendix A.

Table A.4: List of identified underground carding forums

Forum Name	**Forum Address**	**Forum Name**	**Forum Address**
Agorafoum	Lacbzxobeprssfx.onion	Bus1nexx	Bus1nezz.biz
Altenen	Altenen.com	Cardingmafia	Cardingmafia.ws
Crdpro	Crdpro.su	Bpcsqad	Bpcsquad.com
Crimenetwork	Crimenc5wxi63f4r.onion	Procarder	Procarder.ru
Cardingforum	Cardingforum.org	Cardersforum	Cardersforum.se
Hackingforum	Hacingforum.ru	Crimes	Crimes.ws
Unixoder	Unixorder.com	Carderbase	Carderbase.su
Crdclub	Crdclub.ws	Carder	Carder.me
Carderscave	Carderscave.ru	Darkstuff	Darkstuff.net
Infraud	Infraud.cc	Coinodeal	Coinodeal.com
Lampeduza	Lampeduza.so	Texedocrew	Tuxedocrew.biz
Blackstuff	Blackstuff.net/forum.php	Privatemarket	Privatemarket.us
Omerta	Omerta.cm	Diamonddumps	Diamonddumps.org